# OCTAVE®-S Implementation Guide, Version 1.0

# Volume 10: Example Scenario

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

*January 2005*

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

# OCTAVE®-S Implementation Guide, Version 1.0

# Volume 10: Example Scenario

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

*January 2005*

**Networked Systems Survivability Program**

This report was prepared for the

SEI Joint Program Office
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

# Table of Contents

# List of Figures

# About This Document

This document is Volume 10 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides complete example scenario of a fictitious medical facility, MedSite, and the results of its OCTAVE-S evaluation. Most of the worksheets showing the example results are provided. However, the complete worksheets for only one asset (rather than five) are included.

The other volumes in this handbook are

- *Volume 1: Introduction to OCTAVE-S* – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- *Volume 3: Method Guidelines* – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- *Volume 8: Critical Asset Workbook for People* – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- ***Volume 10: Example Scenario*** – This volume includes a detailed scenario illustrating a completed set of worksheets.

# Abstract

The Operationally Critical Threat, Asset, and Vulnerability Evaluation$^{SM}$ (OCTAVE$^{®}$) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization’s security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization’s personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization’s unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization’s business and security processes, so it will be able to conduct all activities by itself.

# 1 MedSite Background

To help you understand how to complete the individual steps in this evaluation, we provide an example that illustrates how each step was conducted by personnel in a fictitious small medical facility called MedSite. The first two sections, including this one, provide background on MedSite and a commentary about how the evaluation proceeded at MedSite. The rest of this document consists of OCTAVE-S worksheets showing the results achieved by the MedSite analysis team. The background provides the necessary context to understand the contents of the worksheets and should be read in conjunction with the worksheets.

## 1.1 MedSite Description

MedSite is a hospital with several clinics and labs, some of which are at remote locations. The hospital includes the following functional areas:

- a permanent administrative organization
- permanent and temporary medical personnel, including physicians, surgeons, and medical staff
- permanent and temporary maintenance personnel, including facility and maintenance staff
- a small information technology department (three people) that is responsible for on-site computer and network maintenance and upgrades and for help desk activities (e.g., handling simple user requests)

## 1.2 MedSite's Organizational Structure

The MedSite Administrator is the chief administrator for the hospital. The chief administrator has a small staff that is responsible for overseeing operations at MedSite. Each major functional area of the organization (administrative, medical, and lab) reports directly to the chief administrator. MedSite's senior management team includes the MedSite Administrator and the individuals who lead the functional areas of the organization. Each functional area of MedSite contains one or more operational areas. The head of each operational area is considered to be a middle manager in the organization. Figure 1 shows the organizational chart for MedSite.

## 1.3 MedSite's System

MedSite's main information system is the Patient Information Data System (PIDS). PIDS is a distributed database application and system software with a dedicated PIDS server on a shared network accessed by both dedicated and shared desktop personal computers (PCs). The shared components support a variety of medical applications and databases. The system also links and integrates a set of smaller, older databases related to patient care, lab results, and billing.

Patient data can be entered into PIDS or one of the other databases at any time from any workstation. Physicians, administrative clerks, lab technicians, and nurses have authorization to enter data into PIDS as well as the other systems. Personal computers, or workstations, are located in all offices, treatment rooms (including emergency rooms), nursing stations, and labs. In addition, physicians can also remotely access PIDS using their home personal computers. In fact, there is talk around the hospital that medical personnel will soon be able to access PIDS using personal digital assistants (PDAs).

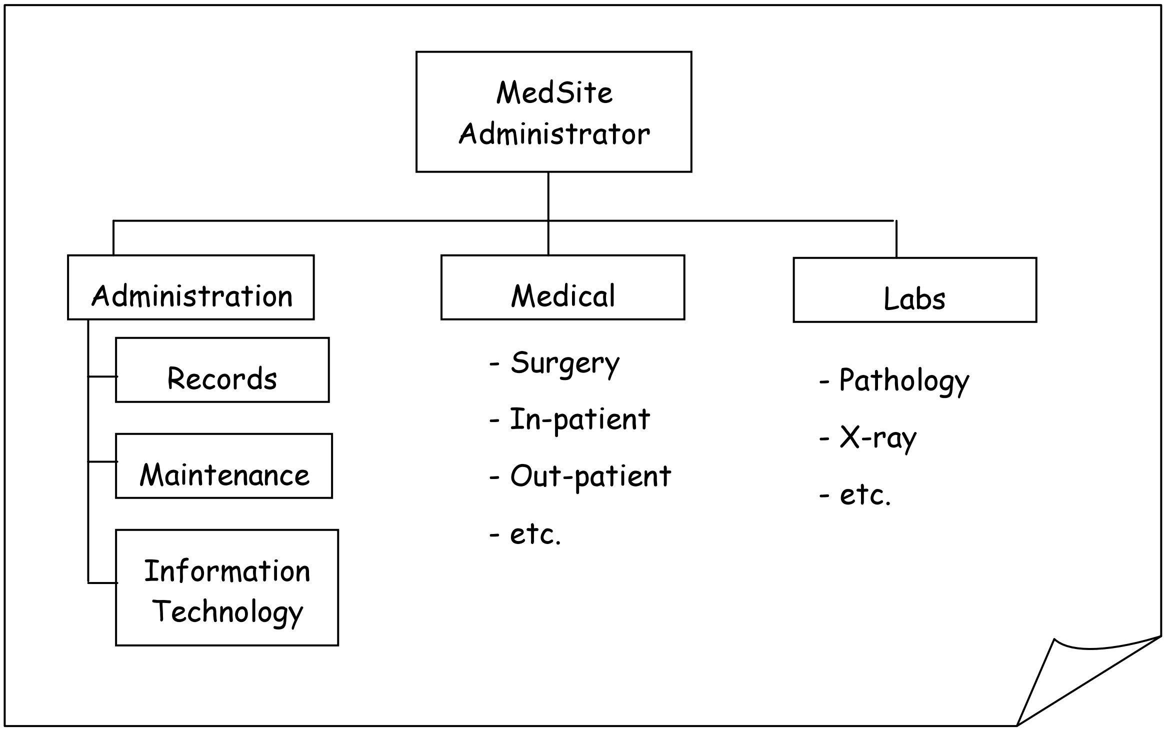


*Figure 1: High-Level MedSite Organizational Chart*

An independent contractor, ABC Systems, provides support for most of the systems at MedSite as well as for the network. MedSite's information technology (IT) personnel provide day-to-day maintenance under the training and direction of ABC Systems personnel. MedSite's IT staff also support the help desk by taking calls and responding to immediate needs. The IT staff members from MedSite provide on-site help desk support and basic system maintenance. ABC Systems provided MedSite's IT personnel with limited systems and network training about a year ago.

MedSite's senior managers decided they wanted a comprehensive review of information security within their facility. Several new regulations are now in effect (e.g., the Health Insurance Portability and Accountability Act [HIPAA]), requiring MedSite to document the results of an information security risk evaluation. The regulations also require MedSite to implement a practice-based standard of due care. After some discussion and consultation with other medical facility managers, they decided to use OCTAVE-S.

The analysis team has been selected and trained. The core analysis team members are

- Alvarez – a physician, at MedSite for five years
- Green – assistant manager of Administration, at MedSite for eight years. Green will lead the analysis team.
- Smith – senior IT staff member, at MedSite for three years
- Haley – lab technician, at MedSite for four years

The team met to prepare for the evaluation. They decided to scope the evaluation to include the entire organization as there are only three real operational areas – Administration, Medical, and the Lab. They also checked with colleagues in other medical facilities to locate any historical data on any type of threats that they might be willing to share later on or to discuss when the analysis team needed to define probability evaluation criteria. Probability is required by some regulations, and the team felt that they needed to try to use some form of qualitative probability during risk analysis.

As this was their first use of OCTAVE-S, they decided not to tailor the catalog of practices or the surveys to align them with current regulations, such as HIPAA. Instead, after the evaluation, they will use a gap analysis to determine what additional actions are required to ensure compliance and to protect their information-related assets. The budget for security improvements over the next six months is limited, and senior managers prefer to ensure their critical assets are protected now and deal with any additional regulation compliance during the next budget cycle.

## 1.4 MedSite Team's Experience

MedSite's analysis team completed the evaluation in four weeks working part time. This section summarizes the team's activities, its decisions, and other contextual information related to the evaluation. As you review the results, you will notice that we provide complete results for only one of the critical assets.

## 1.4.1 Phase 1: Build Asset-Based Threat Profiles

The analysis team met daily over the course of one week to finish Phase 1. At the end of the week, the team met with MedSite's senior managers to review the impact evaluation criteria and get them approved. MedSite's senior managers decided to use the criteria developed by the team and subsequently review the results. If the criteria turned out to be too vague or if they seemed to skew the results, senior managers reserved the right to revise the criteria and ask the team to re-evaluate the risks.

### 1.4.1.1 Process S1: Identify Organizational Information

**S1.1: Establish impact evaluation criteria (Step 1)**

Using the *Impact Evaluation Criteria Worksheet* [p. 33], the analysis team defined the ranges of possible impacts on the organization. The team had sufficient information on the nature of impacts caused by common problems and emergencies, and it used this information as the basis for setting impact measures (high, medium, low) across multiple impact areas. For example, MedSite is a very successful company, with more than 75% of the region's people coming to MedSite for medical care. MedSite normally sees a 5-15% fluctuation in patient numbers from month to month. The team uses this information to determine that the company could recover from a 10% drop in customers, but a 30% drop would mean a serious problem that could be irreversible. MedSite's budget includes a 2% margin for unexpected changes in operating costs and a 5% margin for unexpected changes in overall revenue. Insurance covers nearly all types of losses of up to $250,000 and many items up to $1 million without any increase in premiums. Any coverable loss of more than $1 million means an immediate increase in premiums. In terms of production, minor increases (10% for a few days) in personnel hours happen all the time because of accidents and unexpected fluctuations in patient needs. A high increase occurred during the previous year when a snowstorm nearly paralyzed the community. Nearly everyone at MedSite worked an additional 30% for a 3-day period to make up for lost time. The team also determined that any loss of life or permanent damage to patients was considered unacceptable. These items were incorporated into the evaluation criteria.

**S1.2: Identify organizational assets (Step 2)**

The analysis team used its knowledge of MedSite's systems as a starting point for identifying assets, because staff members' daily tasks were tightly integrated with the systems they used. When using the *Asset Identification Worksheet* [p. 45] to identify assets, team members could see how much information actually resided on MedSite's information systems. Patient information, which was regulated in terms of privacy and security, could be found in several forms including both electronic and paper files. The team also noticed that personal computers were common to all systems and provided a conduit to all important electronic information. It was more difficult for the team to identify people-related assets, because everyone had important roles at MedSite.

Eventually, the team decided that only people with unique skills or knowledge that could not easily be replaced would be documented as assets during the evaluation. They were essentially interested in identifying single points of failure related to people. For example, Smith was the only IT staff member with networking skills and was thus critical to day-to-day operations. Likewise the people at ABC Systems were also identified as important people-related assets. The staff at ABC Systems maintained PIDS for MedSite, and it would be difficult to find any other contracting organization that could easily assume this responsibility without disrupting MedSite's operations. In addition, ABC Systems was also in the midst of developing the replacement for PIDS (PIDS II), making ABC Systems integral to the future operations of MedSite as well.

**S1.3: Evaluate organizational security practices (Steps 3-4)**

The team used the *Security Practices Worksheet* [p. 51] to document the current state and effectiveness of their security practices. Team members discussed each survey question until they arrived at a consensus (Step 3a) about the extent to which each practice was present at MedSite. As they discussed a practice, team members often recorded notes about particular strengths and weaknesses (Step 3b) related to that practice. Finally, for each security practice area, the team assigned it a stoplight status based on the information it recorded (Step 4). The team was surprised at how many areas were assigned red and yellow statuses. Team members did not assign a green status to any of the security practice areas.

The team noted that some security practices were performed well at MedSite, but the vast majority were not executed properly. One of the few practices performed consistently well was documenting and revising policies. Because MedSite's policies were audited periodically, management paid particular attention to this practice area. Unfortunately, medical regulations had not specified the need for security in the past, and MedSite's security-related policies were incomplete. The team believed that physical security practices were adequate and assigned MedSite a yellow status for physical access control. However, monitoring and auditing physical security was assigned a red status. Team members were also concerned that the Facilities Management Group was so independent that it functioned like a separate entity, providing little communication and insight into its actions. After discussing the Facilities Management Group's physical security practices, the analysis team decided to add an additional concern to the collaborative security management security practice area.

Because ABC Systems maintained and controlled PIDS and other systems, the team had a difficult time answering some of the technology-based survey questions. In fact, no one at MedSite really understood what ABC Systems was doing, driving home how dependent MedSite had become on that contracting organization. Team members were also becoming increasingly concerned over the in-progress development of PIDS II.

Even though the majority of answers for the incident management area were negative, this was one area in which MedSite had a good set of documented procedures. The procedures were a standard, tested, and verified set provided by a medical society to which MedSite belonged. As a result, the team gave the company a yellow status for that area.

No other notes or action items resulted from Process S1.

### 1.4.1.2 Process S2: Create Threat Profiles

**S2.1: Select Critical Assets (Steps 5 – 9)**

Selecting critical assets proved to be less difficult that the analysis team expected. The team selected the following critical assets:

- PIDS (Patient Information Data System) – This was an obvious choice for the team. PIDS is central to MedSite's medical operations, because it is the central repository for patient-identifiable information. In addition, MedSite must comply with regulations for protecting the privacy of and securing electronic patient information.
- Paper medical records – These records are somewhat less important than PIDS, because MedSite is trying to move away from its reliance on paper medical records. However, the migration will take several years. In the meantime, the team decided that paper records also constituted a critical asset, because those records contain patient-identifiable information and are subject to privacy regulations.
- ABC Systems – MedSite has become reliant upon the information technology (IT) services provided by ABC Systems, MedSite's main IT contractor. ABC Systems maintains PIDS and other systems for MedSite and is also developing PIDS II, the replacement for PIDS. ABC Systems was an obvious choice as a critical asset given the importance of PIDS, PIDS II, and MedSite's ongoing efforts to become a paperless environment. ABC Systems is also typical of other types of contracting done by MedSite.
- Personal computers (PCs) – The analysis team noted that personal computers were common to all systems, providing a conduit to all important electronic information.
- ECDS (Emergency Care Data System) – This system was selected because it is representative of many smaller systems used at MedSite.

The analysis team recorded its choices for critical assets on the *Critical Asset Selection Worksheet* [p. 83].The team then started a *Critical Asset Workbook* for each critical asset (Step 6). It also recorded its rationale for selecting each asset (Step 7) as well as who uses and is responsible for each critical asset (Step 8) on each asset's *Critical Asset Information Worksheet* [p. 87]. Information about asset relationships had already been recorded on the *Asset Identification Worksheet* and was transcribed to the *Critical Asset Information Worksheet* (Step 9).

### S2.2: Identify security requirements for critical assets (Steps 10 – 11)

Team members discussed which qualities of each asset were important to protect. This discussion resulted in the identification of security requirements for each critical asset, which were recorded on the appropriate *Critical Asset Information Worksheets* (Step 10) [p. 87]. Selecting the most important security requirement was frequently difficult, requiring significant discussion. For example, team members spent a lot of time discussing which security requirement for PIDS was most important (Step 11). After a healthy debate, the team selected availability of patient information as the most important security requirement for PIDS because the health and safety of patients require immediate and continuous access to patient information on PIDS. Confidentiality was also considered to be important, but it lacked the life and health implications of availability. Most of the issues surrounding confidentiality were actually related to regulations. The team decided that when making tradeoffs, the availability of medical information ultimately trumped violations of privacy laws.

### S2.3: Identify threats to critical assets (Steps 12 – 16)

The analysis team then began constructing a threat profile for each critical asset, recording the profile on the appropriate *Risk Profile Worksheets* [pp. 91 and 131]. Team members consulted the appropriate *Threat Translation Guide* (Volumes 5-8) to ensure they actually understood the implied threats. For PIDS (using Volume 6 for systems assets), the team believed that all of the branches for the *human actors using network* and *physical access* trees were active, non-negligible threats (Step 12). Team members came to this conclusion based on their experiences and known issues related to network and physical security. The team believed that most threats from the *system problems* category would typically affect only the availability of information on PIDS. The exception to this was malicious code, which could result in any outcome. Threats from the *other problems* category were also believed to affect only the availability of PIDS.

For ABC Systems, the nature of the threats was quite different, because it is a different type of asset (people) than PIDS (system). The team was really concerned about only one type of threat – not having qualified, timely support from ABC Systems personnel. This was the only threat that the team recorded for ABC Systems.

For PIDS, the team identified the types of people who might be considered threat actors (Step 13). The team documented a broad range of potential actors, including hackers, disgruntled employees, and ABC Systems’ personnel. With no insight into how ABC Systems handled access to confidential information or violations of security, the team was concerned about the potential threat posed by that contractor’s employees. Team members were also concerned about the lax behavior of many staff members at MedSite, especially regarding casual and loose conversations about patients. Smith acknowledged that the limitations of space and funding had resulted in extremely tight working conditions that virtually forced most admissions staff to share passwords and accounts just to get their jobs done in a reasonable amount of time. Employees constituted a strong source of a range of accidental incidents.

With the exception of disgruntled employees, the team determined that the motivation of insiders was generally low (Step 14). Outsiders' motives were difficult to estimate, but the team did feel that being a small, relatively anonymous medical organization made MedSite a less attractive target for outsiders. The team decided that the motives of outsiders were low.

The team decided to talk to a few knowledgeable staff members at MedSite and ABC Systems to determine the known history for some of the threats (Step 15). ABC Systems had some data, but they were not comprehensive. In fact, given the lack of tangible data produced by people from ABC Systems, analysis team members became concerned about what ABC Systems was doing to monitor PIDS and other systems. The team member with information technology experience knew enough to be skeptical of ABC Systems' network monitoring practices. The team recorded a recommendation to the *Notes and Recommendations Worksheet* [p. 17] to verify what ABC Systems was doing to monitor MedSite's systems and networks. The team also marked its confidence in this historical data as low.

Specific areas of concern were recorded on the *Risk Profile Worksheets* (Step 16) [pp. 91 and 131] whenever the team had a particular example or historical incident relative to a threat. For example, it was well-known that staff members occasionally looked up patient information about their friends and relatives, violating privacy. In addition, the physical configuration of offices and the inclusion of workstations in patient rooms also led to many privacy violations. Alvarez mentioned that physicians were still having a hard time remembering to log off PIDS when they left a treatment room. All team members also noted PIDS' notorious history of failing at inopportune times. Finally, the team was concerned that ABC Systems did not really understand either the general needs of a medical facility or the effects of the new privacy and security regulations.

All actions items from Process S2 were documented on the *Action List Worksheet* [p. 27].

## 1.4.2 Phase 2: Identify Infrastructure Vulnerabilities

The analysis team met daily over the course of a few days to complete Phase 2. Team members performed a cursory examination of how people at MedSite accessed critical assets via the organization's networks. The team also reviewed the extent to which security was considered when configuring and maintaining MedSite's computers and networks. Because people at MedSite had little insight into what ABC Systems was doing to configure and maintain MedSite's systems and networks, the team decided to record a recommendation (see *Notes and Recommendations Worksheet* [p. 17]). The recommendation called for MedSite's IT staff to work more closely with ABC Systems after the evaluation to communicate MedSite's security requirements to ABC Systems and to verify that those requirements were being met.

#### 1.4.2.1 Process S3: Examine the Computing Infrastructure in Relation to Critical Assets

**S3.1: Examine access paths (Steps 17 – 18)**

The analysis team used the *Network Access Paths Worksheet* [p. 139] as it reviewed how people accessed MedSite's critical assets. The team noted that PIDS was its own system of interest (Step 17). It also noted that ECDS was its own system of interest, while PCs included all major systems as their systems of interest. Neither ABC Systems nor the paper medical records were reviewed during this phase, because network attacks are irrelevant to these types of assets.

For PIDS, the analysis team identified key classes of components that were part of or related to PIDS. This activity included a cursory examination of internal and external access points for PIDS (Step 18). Team members had different views of what constituted the PIDS system. After much discussion, they agreed that PIDS included server A and on-site workstations (Step 18a). They then looked at how people typically accessed PIDS. The team determined that people used on-site workstations, laptops, PDAs, and home workstations to access PIDS (Step 18c). The team decided that intermediate access points included both internal and external networks (Step 18b) and that PIDS information was stored both locally and off-site (Step 18d). Finally, the team determined that other systems, most notably ECDS and the Financial Record Keeping System (FRKS), also automatically accessed information from PIDS (Step 18e).

**S3.2: Analyze technology-related processes (Steps 19 – 21)**

This activity requires an analysis team to assume an infrastructure point of view when analyzing information. MedSite's team documented the key classes of components (Step 19a) and then noted which critical assets were related to each key class (Step 19b). The team then determined who was responsible for maintaining and securing each key class (Step 20). Where MedSite's own IT personnel were responsible for day-to-day operations, they could make an estimate of how secure the component classes were (Step 21). Many classes, however, were maintained by ABC Systems, and the level of security for those classes was unknown. The analysis team recorded this information on the *Infrastructure Review Worksheet* [p. 143].

Overall, the security of most classes of components was not consistently known. The team recorded some general recommendations to pursue the relationship with ABC Systems and work towards more formal vulnerability testing with them on the *Notes and Recommendations Worksheet* [p. 17].

Finally, the team reviewed the *Risk Profiles* for PIDS, ECDS, and PCs [pp. 91 and 131] as well as the *Security Practices Worksheet* [p. 51], looking to refine information on those worksheets based on the team's Phase 2 analysis. Team members decided there were no changes to the threat trees, just more validation for the concerns already identified. They did add an additional area of concern on the *Risk Profile Worksheet* (Step 16) [p. 131] about ABC Systems personnel not only having access to patient information but also being able to destroy it.

The IT team member also brought up the concern that what he observed on a daily basis did not support ABC Systems' statements that it kept up with vulnerability testing and patches. The team recorded this observation on the *Security Practices Worksheet* [p. 51] as an example of what MedSite's contractor was not doing well.

No other action items, notes, or recommendations from Process S3 were identified.

## 1.4.3 Phase 3: Develop Security Strategy and Plans

The analysis team added an additional team member to help with the development of mitigation plans in Process S5. The new team member had a lot of expertise in problem solving as well as developing plans, budgets, and schedules for MedSite. To ensure that she developed an understanding of the evaluation, the new team member observed Process S4.

### 1.4.3.1 Process S4: Identify and Analyze Risks

**S4.1: Evaluate impact of threats (Step 22)**

The analysis team used the *Impact Evaluation Criteria* [p. 33] they developed during Process S1 to evaluate the impacts of the threats on the organization. The team recorded all impact values on the *Risk Profile Worksheets* [pp. 91 and 131]. Team members considered the health and safety of patients to be the most important criteria, with the remaining criteria all being equal to each other. The team had some difficulty estimating the impacts to productivity and reputation for a few of the threats and decided to get additional help. Team members identified key people with experience in legal matters, public relations, and nursing to help the team estimate the values for certain threats. Together, they all reviewed each area of concern and talked about the types of specific actions that would have to be taken to deal with a realized threat, providing a basis for estimating the actual level of impact (high, medium, low). In particular, team members looked for any threats that might result in physical harm or death to patients. The team also noted on the *Notes and Recommendations Worksheet* [p. 17] that the evaluation criteria should be more broadly reviewed and approved by management.

### S4.2: Establish probability evaluation criteria (Step 23)

The team defined MedSite's probability evaluation criteria using the *Probability Evaluation Criteria Worksheet* [p. 149]. It relied on its experience and expertise as well as the limited historical information it had for threats. Team members reviewed the known histories of threats recorded on the *Risk Profile Worksheets* [pp. 91 and 131] when setting probability measures (high, medium, low). When defining the criteria, the team also referenced historical data about certain types of threats commonly used by other medical organizations when assessing risk.

### S4.3: Evaluate probabilities of threats (Step 24)

Using the *Probability Evaluation Criteria* [p. 149], the team evaluated the probability of each active threat occurring by using the contextual information they had previously recorded on the *Risk Profile Worksheets* (Steps 13-16) [pp. 91 and 131]. Because they had low confidence in their historical estimations for network-based threats, team members lacked confidence in their probability estimates for those types of threats. However, for a few threats, such as unauthorized insiders accidentally viewing information via systems and networks, team members were quite confident that the probability was high because of the known history of such actions. Because it had minimal confidence in many of its probability estimates, the team decided to use probability only as a tie-breaker when selecting risks for mitigation. Impact would be the primary decision-making driver. The team recorded estimates for probability for all active risks on the *Risk Profile Worksheets* [pp. 91 and 131].

No additional actions, notes, or recommendations were identified during Process S4.

## 1.4.3.2 Process S5: Develop Protection Strategy and Mitigation Plans

### S5.1: Describe current protection strategy (Step 25)

The analysis team reviewed the *Security Practices Worksheet* [p. 51] that it completed earlier in the evaluation. Team members transcribed the stoplight status for each area to the *Protection Strategy Worksheets* [p. 153]. They then discussed the current practices and vulnerabilities identified in each practice area. The team noted that the protection strategy and the security practices survey examine two different facets of security practice areas. The protection strategy describes the processes used to perform activities in each security practice area, focusing on the extent to which processes are formally defined. On the other hand, the stoplight status on the security practices survey indicates how well the team believes its organization is performing in each area. Team members noted that an organization could be performing very well in an area, but have very informal processes. Likewise, an organization could have significant room for improvement despite having very formal policies and procedures. They defined the current protection strategy for the organization and recorded the results on the *Protection Strategy*

*Worksheets* [p. 153]. The protection strategy, along with stoplight status information, provided team members with a broad view of MedSite's overall approach to security and the extent to which it was working.

### S5.2: Select mitigation approaches (Steps 26 - 27)

The team transcribed the stoplight statuses from the *Security Practices Worksheet* [p. 51] to the *Risk Profile Worksheets* (Step 26) [pp. 91 and 131], illustrating the current status of each security practice area in relation to the active risks. Before proceeding, the analysis team needed to agree upon the criteria for making decisions. Team members decided that they would look to mitigate risks meeting the following criteria:

- **risks affecting the health and safety of MedSite's patients (i.e., risks with a high impact value for the "Safety" impact area). Reputation and financial impacts were considered to be secondary factors.**
- **risks affecting the most important security requirement (Step 10) of the asset (e.g., availability of PIDS)**
- **risks linked to specific areas of concern about the asset**

Because it had little confidence in many if its probability estimates, the team decided to use probability as a tie-breaker when comparing two similar risks. Team members reviewed the *Risk Profile Worksheet* for each critical asset [pp. 91 and 131], focusing on potential impacts of risks in relation to stoplight statuses. The analysis team was initially overwhelmed. It had assigned nine security practice areas "red" stoplight statuses and six security practice areas "yellow" stoplight statuses. However, the team did not assign a "green" stoplight status to any area. Based on its decision-making criteria, the team looked across all critical assets and decided which risks it would mitigate. Next it decided which risks it could accept. All remaining risks were designated to be deferred and revisited at a later date. The analysis team decided to recommend (on the *Notes and Recommendations Worksheet* [p. 17]) that all deferred risks be looked at again a month after the end of the evaluation.

To mitigate the risks, the team selected the following security practice areas as mitigation areas:

- Security Awareness and Training **– The analysis team believed that their security awareness training did not adequately prepare personnel to handle the day-to-day security issues that arise. Improving this area should reduce the accidental, inside threat sources.**
- Collaborative Security Management **– ABC Systems provided support for managing the network and most of the systems at MedSite, including PIDS. ABC Systems also conducted periodic vulnerability evaluations of MedSite's computing infrastructure. The analysis team was concerned about MedSite's procedures for working with ABC**

**Systems. The team believed that ABC Systems might not be meeting MedSite's information security requirements. Many unanswered questions and ambiguities arose during Process S3, so the team recommended that MedSite review and revise its procedures for working with ABC Systems. With respect to physical security, the Facilities Management Group was responsible for physically securing MedSite's building. No one at MedSite has been formally working with the staff from Facilities Management group. Because of this, the team recommended that the organization review and revise procedures for working with the Facilities Management Group.**

- Monitoring and Auditing Physical Security **– There was some concern by team members that physical security problems existed at MedSite and were not being handled by the Facilities Management Group. The team identified several risks with potentially high impact to the health and safety of patients based on physical access by internal and external threat actors. The team decided that practices related to *Physical Access Control* were adequate. However, practices related to *Monitoring and Auditing Physical Security* required significant improvement. For this reason, *Monitoring and Auditing Physical Security* was selected as a mitigation area. However, because third parties were involved in monitoring and auditing physical security for MedSite, there was some overlap with the *Collaborative Security Management* security practice area.**
- Authentication and Authorization **– MedSite was not using a consistent means of controlling access to its systems and networks (e.g., role-based management of accounts). Staff members inherited far too many access privileges over time. The team was concerned about the potential consequences of these issues. For example, disgruntled staff members could abuse this increased access to affect the availability of PIDS or to modify medical information.**

The team documented its rationale for selecting each area on the *Notes and Recommendations Worksheet* [p. 17]. It also circled mitigation areas on the appropriate *Risk Profile Worksheets* [pp. 91 and 131] that reduce risks designated as "mitigate." Despite its own earlier recommendation to look at *Vulnerability Management* as a mitigation area, the team decided that the improvements in the *Collaborative Security Management* area could mitigate a greater number of risks related to the computing infrastructure than could improvements in *Vulnerability Management*.

### S5.3: Develop risk mitigation plans (Step 28)

The team developed mitigation plans for each selected area using the *Mitigation Plan Worksheets* [p. 181]. The plan for each selected security practice area includes specific activities designed to mitigate specified risks. Some of the mitigation activities were quite broad in nature. For example, one mitigation activity indicated that periodic security awareness training should be provided for all employees once a year. Other mitigation activities were more focused in nature. For example, one mitigation activity specified that IT staff members receive training in particular technologies. This activity did not address training across all technologies, only for a selected few. As it defined each mitigation activity, the team also recorded its rationale for that particular activity (what was it mitigating or improving), who should be responsible for the activity, and any additional management action that might be required to implement that activity.

### S5.4: Identify changes to protection strategy (Step 29)

The analysis team reviewed the *Protection Strategy Worksheets* [p. 153] to note any changes triggered by mitigation activities. For example, the mitigation activity that called for security awareness training for all employees once a year triggered a change in MedSite's protection strategy. The protection strategy previously required security awareness training only for new employees. On the other hand, the mitigation activity that specified training in particular technologies for IT staff members did not trigger a change in MedSite's protection strategy because the activity did not address training for all technologies. This activity simply improved how one aspect of MedSite's protection strategy was implemented.

Next, the team reviewed the protection strategy, looking for any additional changes to the strategy that it wanted to make. It immediately focused on the *Security Policies and Regulations* area. MedSite had a partial set of documented security-related policies. Because MedSite would soon be required to comply with new data security regulations, the team decided that procedures for complying with those regulations would need to be created. It marked that change to the protection strategy. Team members also noted that while some security-related policies existed, few staff members understood them. Since security awareness training was already being updated, the team decided to include information about MedSite's security policy in that training. Finally, the team decided to address policy enforcement. Even if people knew about and understood MedSite's security policy, their behaviors would change only if they also knew that management was enforcing that policy. Thus, the team decided that procedures for enforcing MedSite's policy needed to be created. The team then developed a mitigation plan to implement the changes to the *Security Policies and Regulations* area. In the rationale area for each mitigation activity, the team noted that these activities were driven by general concerns and regulations, rather than by specific risks.

The analysis team also identified the following two action items during Process S5, documenting them on the *Action List Worksheet* [p. 27]:

- ***Resend basic security policy reminders.* The IT department had sent emails to all staff in the past regarding basic security policy issues. Because improving MedSite's security awareness and training program was seen as a long-term initiative, this action item provided a short-term awareness mechanism without much investment.**
- ***Change the physical configuration of the admissions office.* One of the physical security problems identified during the evaluation was the physical configuration of the admissions area. Most workstations were directed toward public areas, where patients**

**and staff could see medical information on the screens of those workstations. To protect the privacy of medical and admissions information, the analysis team decided to recommend changing the configuration of the admissions office to ensure that workstations could not be easily seen by people passing through the admissions area.**

### S5.5: Identify next steps (Step 30)

Using the *Next Steps Worksheet* [p. 195], the team identified several items required to support implementation of OCTAVE-S results. First, senior management needed to make information security a priority and not a back-burner issue. Second, adequate funding to implement the mitigation plans, protection strategy changes, and action items needed to be allocated. The team also noted that the following items would need to be completed within the next month.

- **People who had been assigned responsibility for implementing a mitigation plan will provide a *detailed* implementation plan for review.**
- **All deferred risks will be reviewed.**
- **The analysis team will compare the security practice surveys to regulations (including HIPAA) to determine if there are any additional practices that need to be added or improved to comply with current regulations.**

The team also recommended conducting another OCTAVE-S evaluation in about 12-18 months, providing sufficient time to implement the recommendations from the evaluation it had just completed.

# 2 Notes and Recommendations Worksheet

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| With no indications that we have been externally attacked, we don't know if the reason is that we really haven't been attacked or that no one is monitoring the right things to determine if we have been. | Step __12__ |

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| | Step _______ |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| We need a way to determine what ABC Systems is doing to monitor for external attacks. This may require a contractual discussion. | Step __15___ |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| We need a more formal or increased communication with ABC Systems. | Step __21___ |

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| We do not believe vulnerability management is being adequately performed on PIDS. | Step __21__ |

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| | Step _______ |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| The ability to manage vulnerabilities should be a candidate for a risk mitigation plan in Phase 3. This may also be more of ABC Systems' responsibility than ours. | Step __27___ |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| Security Awareness and Training is selected as a mitigation area.<br>Rationale: MedSite's security awareness training does not adequately address the security issues that staff members face on a daily basis. Improving this area would help to address several risks with a high safety impact linked to accidental actions by staff members. | Step __27___ |

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| | Step _______ |

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| | Step _______ |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| Collaborative Security Management is selected as a mitigation area.<br>Rationale: ABC Systems provides support for managing the network and most of the systems at MedSite, including PIDS. ABC Systems also conducts periodic vulnerability evaluations of MedSite's computing infrastructure. ABC Systems might not be meeting MedSite's information security requirements. Since ABC Systems plays such a vital role in configuring, maintaining, and securing MedSite's computing infrastructure, procedures for working with ABC Systems should be reviewed and revised. | Step __27___ |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| Monitoring and Auditing Physical Security is selected as a mitigation area.<br>Rationale: There is concern that physical security problems exist at MedSite. The team identified several risks with potentially high impact to the health and safety of patients based on physical access by internal and external threat actors. However, the team does not have enough information to determine exactly how to address the issue. Conducting a physical security audit will characterize the extent of the problem. | Step __27___ |

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| | Step _______ |

**Note**

| | |
|---|---|
| *What notes do you want to record?*<br>*Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.* | *For which step is this note relevant?* |
| | Step _______ |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| Authentication and Authorization is selected as a mitigation area.<br>Rationale: MedSite is currently not using role-based management of accounts. In addition, staff members inherit far too many access privileges over time. The team is concerned about the potential consequences of these issues. For example, disgruntled staff members could abuse this increased access to modify information. | Step 27 |

**Recommendation**

| | |
|---|---|
| *What recommendations do you want to record?* | *For which step is this recommendation relevant?* |
| Look at all deferred risks again in 30 days. | Step 26 |

# 3 Action List Worksheet

**Action Item**

| | | |
|---|---|---|
| | *What actions do you intend to take?*<br>*Assign an identification number to each action item.* | *For which step is this action item relevant?* |
| ID # ___1___ | Ask ABC systems what other medical-related customers they have and if we could talk to them. | Step __13___ |

**Action Item**

| | | |
|---|---|---|
| | *What actions do you intend to take?*<br>*Assign an identification number to each action item.* | *For which step is this action item relevant?* |
| ID # ___2___ | Look for other vendors in this vicinity who could be candidates for taking over our systems should we need an alternative vendor. Check medical conferences and society meetings/seminars. | Step __13___ |

## Action Item

*What additional information do you want to document for each action item?*

*Record additional information below.*

**Responsibility:** *Who is responsible for completing the action item?*

Administration – contract manager

**Completion Date:** *By when must the action item be completed?*

Within the next 2 weeks

**Additional Support:** *What additional support (by management or others) is required to complete the action item?*

## Action Item

*What additional information do you want to document for each action item?*

*Record additional information below.*

**Responsibility:** *Who is responsible for completing the action item?*

Analysis team members and a few others who attend conferences and seminars.

**Completion Date:** *By when must the action item be completed?*

Within the next 6 months

**Additional Support:** *What additional support (by management or others) is required to complete the action item?*

**Action Item**

| | | |
|---|---|---|
| | *What actions do you intend to take?*<br>*Assign an identification number to each action item.* | *For which step is this action item relevant?* |
| ID #<br>___3___ | Resend basic security policy reminders. | Step __29___ |

**Action Item**

| | | |
|---|---|---|
| | *What actions do you intend to take?*<br>*Assign an identification number to each action item.* | *For which step is this action item relevant?* |
| ID #<br>___4___ | Change the physical configuration of the admissions office. | Step __29___ |

**Action Item**

| | |
|---|---|
| | *What additional information do you want to document for each action item?*<br>*Record additional information below.* |
| **Responsibility:** | *Who is responsible for completing the action item?*<br>IT Group |
| **Completion Date:** | *By when must the action item be completed?*<br>Within the next 2 weeks |
| **Additional Support:** | *What additional support (by management or others) is required to complete the action item?*<br>MedSite's CIO needs to approve this action item and assign it to someone in the IT group. |

**Action Item**

| | |
|---|---|
| | *What additional information do you want to document for each action item?*<br>*Record additional information below.* |
| **Responsibility:** | *Who is responsible for completing the action item?*<br>Facilities Management |
| **Completion Date:** | *By when must the action item be completed?*<br>Within the next month |
| **Additional Support:** | *What additional support (by management or others) is required to complete the action item?*<br>MedSite's management team needs to approve this action item and assign it to the Facilities Management Group. |

# 4 Impact Evaluation Criteria Worksheet

## Step 1

**Step 1**

**Reputation/Customer Confidence**

| Impact Type | Low Impact |
|---|---|
| *Reputation* | Reputation is minimally effected; little or no effort or expense is required to recover. |
| *Customer Loss* | Less than __10__% reduction in customers due to loss of confidence |
| *Other:* | |
| *Other:* | |

**Reputation/Customer Confidence**

| Medium Impact | High Impact |
|---|---|
| Reputation is damaged, and some effort and expense is required to recover. | Reputation is irrevocably destroyed or damaged. |
| __10__to __30__% reduction in customers due to loss of confidence | More than __30__% reduction in customers due to loss of confidence |
| | |
| | |

**Step 1**

**Financial**

| **Impact Type** | **Low Impact** |
|---|---|
| *Operating Costs* | Increase of less than ___2___% in yearly operating costs |
| *Revenue Loss* | Less than ___5___% yearly revenue loss |
| *One-Time Financial Loss* | One-time financial cost of less than $__250,000__ |
| *Other:* | |

**Financial**

| Medium Impact | High Impact |
|---|---|
| Yearly operating costs increase by ___2___to __15___% | Yearly operating costs increase by more than __15___% |
| ___5___to ___20__% yearly revenue loss | Greater than ___20__% yearly revenue loss |
| One-time financial cost of $__250,000__ to $_1 million __ | One-time financial cost greater than $_1 million __ |
| | |

**Step 1**

**Productivity**

| **Impact Type** | **Low Impact** |
|---|---|
| *Staff Hours* | Staff work hours are increased by less than __10_% for _______~~to~~ __2__ day(s). |
| *Other:* | |
| *Other:* | |
| *Other:* | |

**Productivity**

| Medium Impact | High Impact |
|---|---|
| Staff work hours are increased between __10_% and __30_% for ~~_______to~~ __2__ day(s). | Staff work hours are increased by greater than __30_% for ~~_______to~~ __2__ day(s). |
| | |
| | |
| | |

**Step 1**

**Safety/Health**

| **Impact Type** | **Low Impact** |
|---|---|
| *Life* | patients'<br>No loss or significant threat to ~~customers' or staff members'~~ lives |
| *Health* | Minimal, immediately treatable degradation in ~~customers' or staff members'~~ health with recovery within four days patients' |
| *Safety* | Safety questioned |
| *Other:* | |

| | **Safety/Health** |
|---|---|
| **Medium Impact** | **High Impact** |
| Patients’<br>~~Customers’ or staff members’~~ lives are threatened, but they will recover after receiving medical treatment. | patients’<br>Loss of ~~customers’ or staff members’~~ lives |
| Temporary or recoverable impairment of ~~customers’ or staff members’~~ health<br>patients’ | Permanent impairment of significant aspects of ~~customers’ or staff members’~~ health<br>patients’ |
| Safety affected | Safety violated |
| | |

**Step 1**

**Fines/Legal Penalties**

| **Impact Type** | **Low Impact** |
|---|---|
| *Fines* | Fines less than $__10,000___ are levied. |
| *Lawsuits* | Non-frivolous lawsuit(s) less than $_100,000__ are filed against the organization or frivolous lawsuit(s) are filed against the organization. |
| *Investigations* | No queries from government or other investigative organizations. |
| *Other:* | |

|  | **Fines/Legal Penalties** |
|---|---|
| **Medium Impact** | **High Impact** |
| Fines between $__10,000___ and $_100,000__ are levied. | Fines greater than $_100,000__ are levied. |
| Non-frivolous lawsuit(s) between $_100,000__ and $_1 million __is filed against the organization. | Non-frivolous lawsuit(s) greater than $_1 million __is filed against the organization. |
| Government or other investigative organization requests information or records (low profile). | Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices. |
|  |  |

# 5 Asset Identification Worksheet

## Step 2

**Step 2**

**Information, Systems, and Applications**

| **System** | **Information** |
|---|---|
| *What systems do people in your organization need to perform their jobs?* | *What information do people in your organization need to perform their jobs?* |
| Patient Information Data System (PIDS) | – patient medical information |
| Financial Record Keeping System (FRKS) | – billing records<br>– insurance records<br>– payment schedules |
| Emergency Care Data System (ECDS) | – billing records<br>– insurance records |
| personal computers | – patient medical information<br>– billing records<br>– insurance records<br>– payment schedules<br>– providers' credentials (paper files) |
| email server (for general email) | – information in emails<br>– patient information (exchanges among doctors) |

| | **Information, Systems, and Applications** |
|---|---|
| **Applications and Services** | **Other Assets** |
| *What applications and services do people in your organization need to perform their jobs?* | *What other assets are closely related to these assets?* |
| – database application<br>– email<br>– Internet connectivity | – paper medical records<br>– Internet Service Provider |
| – database application<br>– Internet connectivity | – Internet Service Provider |
| – Internet connectivity | – Internet Service Provider |
| • email<br>– Internet connectivity | – PIDS<br>– FRKS<br>– ECDS<br>– other functional systems<br>– Internet Service Provider |
| | – PIDS<br>– personal computers |

Step 2

**People**

| **People** | **Skills and Knowledge** |
|---|---|
| *Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?* | *What are their special skills or knowledge?* |
| External relations | A group of people who controls the release of patient medical information |
| ABC Systems | Group that manages all major changes, maintenance, and upkeep of all major systems |
| MTF help desk | PC technicians who troubleshoot PC problems for users |
| Mr. Smith | Senior IT staff member. He is the only on-site staff member with networking skills. |
| | |

| | People |
|---|---|
| **Related Systems** | **Related Assets** |
| *Which systems do these people use?* | *Which other assets do these people use (i.e., information, services or applications)?* |
| – PIDS | |
| – PIDS<br>– FRKS<br>– ECDS<br>– network | |
| – PCs | |
| | |
| | |

# 6 Security Practices Worksheet

## Steps 3a, 3b, and 4

**1. Security Awareness and Training**

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| Staff members understand their security roles and responsibilities. This is documented and verified. | Very Much Somewhat [✓ Not At All] Don't Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Very Much Somewhat [✓ Not At All] Don't Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Very Much Somewhat [✓ Not At All] Don't Know |
| Staff members follow good security practice, such as<br>• securing information for which they are responsible<br>• not divulging sensitive information to others (resistance to social engineering)<br>• having adequate ability to use information technology hardware and software<br>• using good password practices<br>• understanding and following security policies and regulations<br>• recognizing and reporting incidents | Very Much Somewhat [✓ Not At All] Don't Know |

**1. Security Awareness and Training**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| – We have training, guidance, regulations, and policies.<br>– Awareness training is required to get an account. | – There is a lack of training for IT staff.<br>– Awareness training is inadequate.<br>– Staff does not understand security issues.<br>– There is little understanding of security roles and responsibilities.<br>– People share accounts and passwords. | ☒ Red<br>❑ Yellow<br>❑ Green<br>❑ Not Applicable |

## 2. Security Strategy

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** | | | |
|---|---|---|---|---|
| The organization's business strategies routinely incorporate security considerations. | Very Much | Somewhat | [✓ Not At All] | Don't Know |
| Security strategies and policies take into consideration the organization's business strategies and goals. | Very Much | Somewhat | [✓ Not At All] | Don't Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Very Much | [✓ Somewhat] | Not At All | Don't Know |

**2. Security Strategy**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| | – Our current protection strategy is not effective.<br>– Our security strategy lacks business sense. It is not proactive. | ☒ Red<br>□ Yellow<br>□ Green<br>□ Not Applicable |

## 3. Security Management

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** | | | |
|---|---|---|---|---|
| Management allocates sufficient funds and resources to information security activities. | Very Much | [✓ Somewhat] | Not At All | Don’t Know |
| Security roles and responsibilities are defined for all staff in the organization. | Very Much | [✓ Somewhat] | Not At All | Don’t Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Very Much | Somewhat | [✓ Not At All] | Don’t Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Very Much | Somewhat | [✓ Not At All] | Don’t Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Very Much | [✓ Somewhat] | Not At All | Don’t Know |
| The organization manages information security risks, including<br>• assessing risks to information security<br>• taking steps to mitigate information security risks | Very Much | Somewhat | [✓ Not At All] | Don’t Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risks and vulnerability assessments). | Very Much | Somewhat | Not At All | [✓ Don’t Know] |

## 3. Security Management

**Step 3b**

| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** |
|---|---|
| – This risk evaluation is a step in the right direction. | – We have an inadequate budget for security.<br>– Staff members are complacent about security. |

**Step 4**

| **How effectively is your organization implementing the practices in this area?** |
|---|
| ☒ Red<br>□ Yellow<br>□ Green<br>□ Not Applicable |

**4. Security Policies and Regulations**

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** | | | |
|---|---|---|---|---|
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | [✓ Very Much] | Somewhat | Not At All | Don’t Know |
| There is a documented process for management of security policies, including<br>• creation<br>• administration (including periodic reviews and updates)<br>• communication | Very Much | [✓ Somewhat] | Not At All | Don’t Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Very Much | [✓ Somewhat] | Not At All | Don’t Know |
| The organization uniformly enforces its security policies. | Very Much | Somewhat | [✓ Not At All] | Don’t Know |

**4. Security Policies and Regulations**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| – Policies and procedures exist.<br>– There are established incident-handling policies and procedures. | – There is poor communication of policies.<br>– People don't always read and follow policies and procedures.<br>– There is a lack of follow-up on reported violations.<br>– We don't enforce our policies. | □ Red<br>☒ Yellow<br>□ Green<br>□ Not Applicable |

**5. Collaborative Security Management**

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including<br>• protecting information belonging to other organizations<br>• understanding the security polices and procedures of external organizations<br>• ending access to information by terminated external personnel | Very Much [✓ Somewhat] Not At All Don't Know |
| The organization documents information protection requirements and explicitly communicates them to all appropriate third parties. | Very Much Somewhat [✓ Not At All] Don't Know |
| The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements. | Very Much Somewhat [✓ Not At All] Don't Know |
| The organization has policies and procedures for collaborating with all third-party organizations that<br>• provide security awareness and training services<br>• develop security policies for the organization<br>• develop contingency plans for the organization | Very Much [✓ Somewhat] Not At All Don't Know |

**5. Collaborative Security Management**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| | – We rely on more than ABC Systems to support our networks.<br>– There is no single point of contact for the network. Things get confused sometimes.<br>– MedSite does not communicate its security-related requirements for PIDS to ABC Systems. | ☒ Red<br>❑ Yellow<br>❑ Green<br>❑ Not Applicable |

## 6. Contingency Planning/Disaster Recovery

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** | | | |
|---|---|---|---|---|
| An analysis of operations, applications, and data criticality has been performed. | [✓ Very Much] | Somewhat | Not At All | Don't Know |
| The organization has documented, reviewed, and tested<br>• business continuity or emergency operation plans<br>• disaster recovery plan(s)<br>• contingency plan(s) for responding to emergencies | Very Much | [✓ Somewhat] | Not At All | Don't Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Very Much | [✓ Somewhat] | Not At All | Don't Know |
| All staff are<br>• aware of the contingency, disaster recovery, and business continuity plans<br>• understand and are able to carry out their responsibilities | Very Much | [✓ Somewhat] | Not At All | Don't Know |

**6. Contingency Planning/Disaster Recovery**

**Step 3b**

| What is your organization currently doing well in this area? | What is your organization currently *not* doing well in this area? |
|---|---|
| – We have disaster recovery plans for natural disasters and some emergencies. | – We don't have a business continuity plan.<br>– We don't have disaster recovery plans for systems and networks.<br>– We're not sure how much testing has been done of the plans we do have. |

**Step 4**

| How effectively is your organization implementing the practices in this area? |
|---|
| □ Red<br>☒ Yellow<br>□ Green<br>□ Not Applicable |

## 7. Physical Access Control

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | [✓ Very Much] Somewhat Not At All Don’t Know |
| There are documented policies and procedures for managing visitors. | [✓ Very Much] Somewhat Not At All Don’t Know |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Very Much [✓ Somewhat] Not At All Don’t Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Very Much [✓ Somewhat] Not At All Don’t Know |
| ***If staff from a third party is responsible for this area:***<br>The organization’s requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media. | Very Much [✓ Somewhat] Not At All Don’t Know |
| The organization formally verifies that contractors and service providers have met the requirements for physical access control. | Very Much [✓ Somewhat] Not At All Don’t Know |

**7. Physical Access Control**

**Step 3b**

| What is your organization currently doing well in this area? | What is your organization currently *not* doing well in this area? |
|---|---|
| – We are required to lock our offices at the end of the day.<br>– Physical security for our computer room is good. | – Once sensitive information is printed and distributed, it is not properly controlled or handled.<br>– Physical security is hampered by<br>o location/distribution of PCs<br>o need to share PCs<br>o shared office space<br>o sharing codes to cipher locks<br>o multiple access points to rooms |

**Step 4**

| How effectively is your organization implementing the practices in this area? |
|---|
| □ Red<br>☒ Yellow<br>□ Green<br>□ Not Applicable |

## 8. Monitoring and Auditing Physical Security

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>Maintenance records are kept to document the repairs and modifications of a facility's physical components. | Very Much Somewhat [✓ Not At All] Don't Know |
| An individual's or group's actions, with respect to all physically controlled media, can be accounted for. | Very Much Somewhat [✓ Not At All] Don't Know |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. | Very Much Somewhat [✓ Not At All] Don't Know |
| ***If staff from a third party is responsible for this area:***<br>The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media. | Very Much [✓ Somewhat] Not At All Don't Know |
| The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security. | Very Much Somewhat Not At All [✓ Don't Know] |

**8. Monitoring and Auditing Physical Security**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| | – Audit records are spotty. We're not sure that anyone reviews them. | ☒ Red<br>□ Yellow<br>□ Green<br>□ Not Applicable |

## 9. System and Network Management

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>There are documented and tested security plan(s) for safeguarding the systems and networks. | Very Much Somewhat [✓ Not At All] Don't Know |
| Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information). | [✓ Very Much] Somewhat Not At All Don't Know |
| The integrity of installed software is regularly verified. | Very Much [✓ Somewhat] Not At All Don't Know |
| All systems are up to date with respect to revisions, patches, and recommendations in security advisories. | Very Much [✓ Somewhat] Not At All Don't Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Very Much [✓ Somewhat] Not At All Don't Know |
| Changes to IT hardware and software are planned, controlled, and documented. | Very Much [✓ Somewhat] Not At All Don't Know |
| IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges.<br>• Unique user identification is required for all information system users, including third-party users.<br>• Default accounts and default passwords have been removed from systems. | Very Much [✓ Somewhat] Not At All Don't Know |
| Only necessary services are running on systems – all unnecessary services have been removed. | Very Much Somewhat [✓ Not At All] Don't Know |
| Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. | Very Much [✓ Somewhat] Not At All Don't Know |
| ***If staff from a third party is responsible for this area:***<br>The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks. | Very Much [✓ Somewhat] Not At All Don't Know |
| The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management. | Very Much Somewhat [✓ Not At All] Don't Know |

**9. System and Network Management**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| – ABC Systems has a security plan.<br>– We force users to change their passwords regularly.<br>– ABC Systems has reported very few intrusions.<br>– Systems are well protected with passwords.<br>– ABC Systems runs tools from their site. | – MedSite has no documented security plan.<br>– We don't clean up inherited access rights very well.<br>– We're not sure whether ABC Systems keeps up with security notices.<br>– We haven't been trained in the use of the latest system administration tools. | □ Red<br>☒ Yellow<br>□ Green<br>□ Not Applicable |

## 10. Monitoring and Auditing IT Security

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure. | Very Much [✓ Somewhat] Not At All Don’t Know |
| Firewall and other security components are periodically audited for compliance with policy. | Very Much [✓ Somewhat] Not At All Don’t Know |
| ***If staff from a third party is responsible for this area:***<br>The organization’s requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks. | Very Much [✓ Somewhat] Not At All Don’t Know |
| The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security. | Very Much Somewhat [✓ Not At All] Don’t Know |

**10. Monitoring and Auditing IT Security**

**Step 3b**

| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** |
|---|---|
| – ABC Systems does all IT audits.<br>– ABC Systems runs monitoring tools. | – ABC Systems does not report unusual activity to anyone here. |

**Step 4**

**How effectively is your organization implementing the practices in this area?**

□ Red

☒ Yellow

□ Green

□ Not Applicable

## 11. Authentication and Authorization

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections. | Very Much Somewhat [✓ Not At All] Don't Know |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Very Much [✓ Somewhat] Not At All Don't Know |
| Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified. | Very Much Somewhat [✓ Not At All] Don't Know |
| ***If staff from a third party is responsible for this area:***<br>The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services. | Very Much [✓ Somewhat] Not At All Don't Know |
| The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization. | Very Much Somewhat [✓ Not At All] Don't Know |

**11. Authentication and Authorization**

**Step 3b**

| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** |
|---|---|
| – There are policies and procedures for access and control permissions.<br>– Systems are protected well using passwords. | – We're not using role-based management of accounts.<br>– People inherit far too many privileges. |

**Step 4**

**How effectively is your organization implementing the practices in this area?**

☒ Red

❑ Yellow

❑ Green

❑ Not Applicable

## 12. Vulnerability Management

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>There is a documented set of procedures for managing vulnerabilities, including<br>• selecting vulnerability evaluation tools, checklists, and scripts<br>• keeping up to date with known vulnerability types and attack methods<br>• reviewing sources of information on vulnerability announcements, security alerts, and notices<br>• identifying infrastructure components to be evaluated<br>• scheduling of vulnerability evaluations<br>• interpreting and responding to the results<br>• maintaining secure storage and disposition of vulnerability data | Very Much Somewhat Not At All Don't Know |
| Vulnerability management procedures are followed and are periodically reviewed and updated. | Very Much Somewhat Not At All Don't Know |
| Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified. | Very Much Somewhat Not At All Don't Know |
| ***If staff from a third party is responsible for this area:***<br>The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities. | Very Much Somewhat [✓ Not At All] Don't Know |
| The organization formally verifies that contractors and service providers have met the requirements for vulnerability management. | Very Much Somewhat Not At All [✓ Don't Know] |

**12. Vulnerability Management**

**Step 3b**

| What is your organization currently doing well in this area? | What is your organization currently *not* doing well in this area? |
|---|---|
| – ABC Systems does all vulnerability evaluation and management. | – We haven’t received training about how to interpret vulnerability reports. |

**Step 4**

| How effectively is your organization implementing the practices in this area? |
|---|
| ☒ Red<br>□ Yellow<br>□ Green<br>□ Not Applicable |

## 13. Encryption

**Step 3a**

| **Statement** | **To what extent is this statement reflected in your organization?** |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology). | Very Much Somewhat [✓ Not At All] Don't Know |
| Encrypted protocols are used when remotely managing systems, routers, and firewalls. | Very Much Somewhat [✓ Not At All] Don't Know |
| ***If staff from a third party is responsible for this area:***<br>The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies. | Very Much Somewhat Not At All [✓ Don't Know] |
| The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies. | Very Much Somewhat Not At All [✓ Don't Know] |

**13. Encryption**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| | – We don't protect patient information when we send it electronically to third parties.<br>– We don't know whether ABC Systems protects patient information using encryption. The topic has never come up. | ☒ Red<br>□ Yellow<br>□ Green<br>□ Not Applicable |

## 14. Security Architecture and Design

**Step 3a**

| Statement | To what extent is this statement reflected in your organization? |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>System architecture and design for new and revised systems include considerations for<br>• security strategies, policies, and procedures<br>• history of security compromises<br>• results of security risk assessments | Very Much Somewhat [✓ Not At All] Don’t Know |
| The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology. | Very Much [✓ Somewhat] Not At All Don’t Know |
| ***If staff from a third party is responsible for this area:***<br>The organization’s security-related requirements are formally communicated to all contractors and service providers that design systems and networks. | Very Much Somewhat [✓ Not At All] Don’t Know |
| The organization formally verifies that contractors and service providers have met the requirements for security architecture and design. | Very Much Somewhat [✓ Not At All] Don’t Know |

## 14. Security Architecture and Design

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| | – PIDS II is being developed and no one has talked to us about security. | ☒ Red<br>□ Yellow<br>□ Green<br>□ Not Applicable |

## 15. Incident Management

**Step 3a**

| Statement | To what extent is this statement reflected in your organization? |
|---|---|
| ***If staff from your organization is responsible for this area:***<br>Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Very Much [✓ Somewhat] Not At All Don’t Know |
| Incident management procedures are periodically tested, verified, and updated. | Very Much Somewhat [✓ Not At All] Don’t Know |
| There are documented policies and procedures for working with law enforcement agencies. | Very Much Somewhat [✓ Not At All] Don’t Know |
| ***If staff from a third party is responsible for this area:***<br>The organization’s requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services. | Very Much Somewhat Not At All [✓ Don’t Know] |
| The organization formally verifies that contractors and service providers have met the requirements for managing incidents. | Very Much Somewhat Not At All [✓ Don’t Know] |

**15. Incident Management**

| Step 3b | | Step 4 |
|---|---|---|
| **What is your organization currently doing well in this area?** | **What is your organization currently *not* doing well in this area?** | **How effectively is your organization implementing the practices in this area?** |
| – Procedures exist for incident response. | – We have never considered how to deal with law enforcement.<br>– It is not clear how or where we should report incidents.<br>– We have never discussed incident management with ABC Systems. | □ Red<br>☒ Yellow<br>□ Green<br>□ Not Applicable |

# 7 Critical Asset Selection Worksheet

## Step 5

**Step 5**

| | |
|---|---|
| **Questions to Consider:** | *Which assets will have a large adverse impact on the organization if*<br>• *they are disclosed to unauthorized people?*<br>• *they are modified without authorization?*<br>• *they are lost or destroyed?*<br>• *access to them is interrupted?* |

| **Critical Asset** |
|---|
| 1. Patient Information Data System (PIDS) |
| 2. Paper medical records |
| 3. Personal computers |
| 4. ABC Systems |
| 5. Emergency Data Care System (ECDS) |

| Notes |
|---|
| We are dependent on PIDS. |
| The number one data source for patient information is paper medical records. |
| All staff access key medical systems using personal computers. |
| They control our network. |
| This is typical of the 32 functional systems at MedSite. |

# 8 Critical Asset Information Worksheet for Systems

## Steps 6, 7, 8, 9, 10, and 11

Note that from this point on, most of the case scenario results are only for the critical asset PIDS.

| Step 6 | Step 7 |
|---|---|
| **Critical Asset** | **Rationale for Selection** |
| *What is the critical system?* | *Why is this system critical to the organization?* |
| Patient Information Data System (PIDS) | We are 98% dependent on PIDS for delivering patient care. |

**Step 9**

**Related Assets**

*Which assets are related to this system?*

Information:

– Patient medical information

Services and Applications:

– Database

– Email

Other:

– Personal computers

– Paper medical records

– Internet connectivity

– ABC Systems

– External relations

**Step 8**

**Description**

*Who uses the system?* *Who is responsible for the system?*

Providers, lab technician, pharmacists, and appointment schedulers all use PIDS. Each group is responsible for a subset of the medical information on PIDS. ABC Systems has primary responsibility for maintaining PIDS. Some day-to-day maintenance work is performed by our IT staff.

| | | |
|---|---|---|
| **Step 10** | | **Step 11** |
| **Security Requirements** | | **Most Important Security Requirement** |
| *What are the security requirements for this system?*<br>*(Hint: Focus on what the security requirements should be for this system, not what they currently are.)* | | *Which security requirement is most important for this system?* |
| ☒ Confidentiality | Only authorized personnel can view information on ____PIDS______. Information should be restricted to those with a "need to know." Information is subject to the privacy act. | ❑ Confidentiality<br>❑ Integrity |
| ☒ Integrity | Only authorized personnel can modify information on ____PIDS_____. Records must be complete and correct. | ☒ Availability<br>❑ Other |
| ☒ Availability | ______PIDS_____ must be available for personnel to perform their jobs.<br>Access to information is required 24/7.<br>~~Unavailability cannot exceed ______ hour(s) per every ______ hours.~~ | |
| ❑ Other | ______________________________________________<br>______________________________________________ | |

# 9 Risk Profile Worksheets for Systems – PIDS

## Steps 12, 13, 14, 15, 16, 22, 23, 24, 26, 27

## 9.1 Risk Profile Worksheet for PIDS – Human Actors Using Network Access

## Human Actors Using Network Access

## Basic Risk Profile

**Step 12**

**Threat**

*For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.*

*For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.*

**Step 22**

**Impact Values**

*What is the potential impact on the organization in each applicable area?*

| Asset | Access | Actor | Motive | Outcome | Reputation | Financial | Productivity | Fines | Safety | Other |
|---|---|---|---|---|---|---|---|---|---|---|
| PIDS | network | inside | accidental | disclosure | M | M | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |
| | | | deliberate | disclosure | M | M | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |
| | | outside | accidental | disclosure | H | H | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |
| | | | deliberate | disclosure | H | H | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |

**Basic Risk Profile**

**Human Actors Using Network Access**

**Step 24**

**Probability**

*How likely is the threat to occur in the future? How confident are you in your estimate?*

**Step 26**

**Security Practice Areas**

*What is the stoplight status for each security practice area?*

**Step 27**

**Approach**

*What is your approach for addressing each risk?*

| Value | Confidence | Strategic | | | | | | Operational | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Very Much Somewhat Not At All | 1. Sec Training | 2. Sec Strategy | 3. Sec Mgmt | 4. Sec Policy & Reg | 5. Coll Sec Mgmt | 6. Cont Planning | 7. Phys Acc Cntrl | 8. Monitor Phys Sec | 9. Sys & Net Mgmt | 10. Monitor IT Sec | 11. Authen & Auth | 12. Vul Mgmt | 13. Encryption | 14. Sec Arch & Des | 15. Incident Mgmt | Accept | Defer | Mitigate |
| H | \|X----\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|X----\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| H | \|X----\|------\| | [✓ R] | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | [✓ R] | R | R | R | Y | ❑ | ❑ | ☒ |
| L | \|----X\|------\| | [✓ R] | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | [✓ R] | R | R | R | Y | ❑ | ❑ | ☒ |
| L | \|----X\|------\| | [✓ R] | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | [✓ R] | R | R | R | Y | ❑ | ❑ | ☒ |
| L | \|----X\|------\| | [✓ R] | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | [✓ R] | R | R | R | Y | ❑ | ❑ | ☒ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|------\|----X\| | R | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ❑ | ☒ |
| L | \|------\|----X\| | R | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ❑ | ☒ |
| L | \|----X\|------\| | R | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ❑ | ☒ |
| L | \|----X\|------\| | R | R | R | Y | [✓ R] | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ❑ | ☒ |

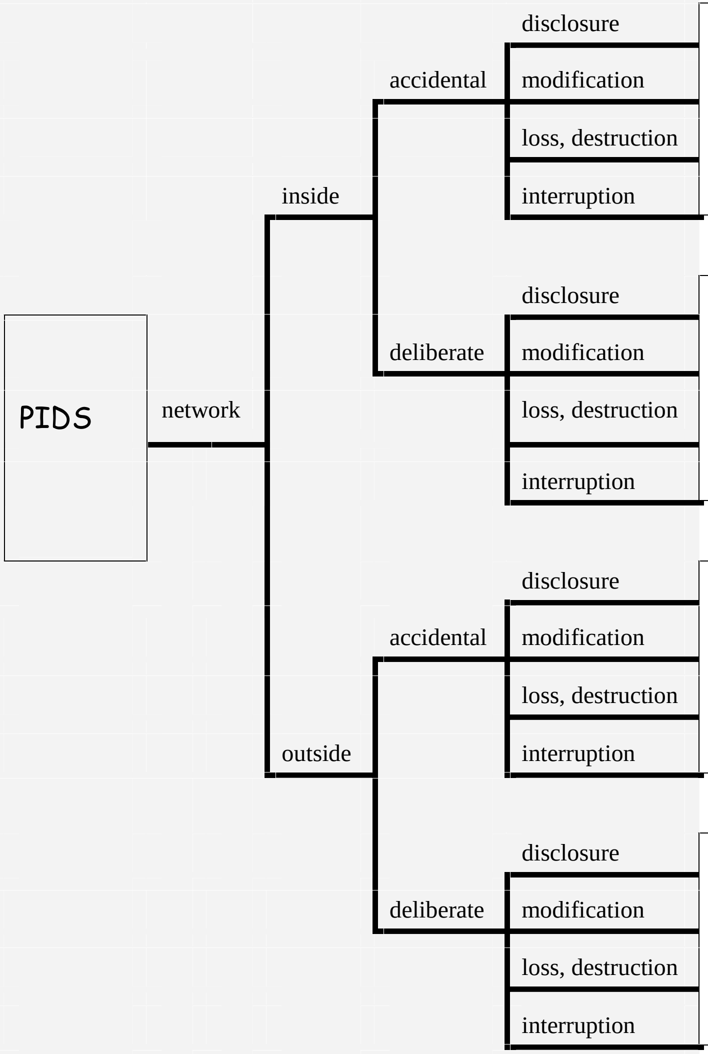
## Human Actors Using Network Access

## Threat Context

**Step 13**

**Threat Actors**

*Which actors pose the biggest threats to this system via the network?*



*Insiders acting accidentally:*

Data entry personnel, medical staff discussing sensitive information in public areas

*Insiders acting deliberately:*

Disgruntled employees, staff misusing PIDS information for non-malicious reasons

*Outsiders acting accidentally:*

ABC Systems

*Outsiders acting deliberately:*

Terrorist, spies, hackers

**Threat Context**

**Human Actors Using Network Access**

| Step 14 | | | | | | Step 15 | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Motive** | | | | | | **History** | | | |
| *How strong is the actor's motive?* | | | *How confident are you in this estimate?* | | | *How often has this threat occurred in the past?* | *How accurate are the data?* | | |
| **High** | **Medium** | **Low** | **Very Much** | **Somewhat** | **Not At All** | | **Very** | **Somewhat** | **Not At All** |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | _10+_ times in ___1__ years | ☒ | ☐ | ☐ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __2___ times in __5___ years | ☐ | ☒ | ☐ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ☐ | ☒ | ☐ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __2___ times in __5___ years | ☒ | ☐ | ☐ |
| ☐ | ☒ | ☐ | ☐ | ☒ | ☐ | __5___ times in __1___ years | ☒ | ☐ | ☐ |
| ☐ | ☐ | ☒ | ☐ | ☒ | ☐ | __0___ times in __5___ years | ☐ | ☒ | ☐ |
| ☐ | ☐ | ☒ | ☐ | ☒ | ☐ | __0___ times in __5___ years | ☐ | ☒ | ☐ |
| ☐ | ☐ | ☒ | ☐ | ☒ | ☐ | __0___ times in __5___ years | ☐ | ☒ | ☐ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ☐ | ☐ | ☒ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ☐ | ☐ | ☒ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ☐ | ☐ | ☒ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ☐ | ☐ | ☒ |
| ☐ | ☐ | ☒ | ☐ | ☒ | ☐ | __0___ times in __5___ years | ☐ | ☐ | ☒ |
| ☐ | ☐ | ☒ | ☐ | ☒ | ☐ | __0___ times in __5___ years | ☐ | ☐ | ☒ |
| ☐ | ☐ | ☒ | ☐ | ☒ | ☐ | __0___ times in __5___ years | ☐ | ☒ | ☐ |
| ☐ | ☐ | ☒ | ☐ | ☒ | ☐ | __0___ times in __5___ years | ☐ | ☒ | ☐ |

Step 16

## Human Actors Using Network Access

**Areas of Concern**

### Insiders Using Network Access

| | |
|---|---|
| Give examples of how *insiders acting accidentally* could use network access to threaten this system. | |
| | |
| Give examples of how *insiders acting deliberately* could use network access to threaten this system. | Staff members with legitimate access to PIDS sometimes use that access to view information that they shouldn't (e.g., medical records of friends). This is a violation of the privacy act. |
| | Disgruntled employees are a concern. The more they know about information technology, the more dangerous they are. |

### Outsiders Using Network Access

| | |
|---|---|
| Give examples of how *outsiders acting accidentally* could use network access to threaten this system. | ABC Systems has access to PIDS and the network. Any deliberate or accidental acts by their staff could affect our ability to provide patient care. |
| | |
| Give examples of how *outsiders acting deliberately* could use network access to threaten this system. | Terrorists and spies are of concern. If they disrupt PIDS, they could shut down MedSite. |
| | Hackers are also a concern. If they disrupt PIDS, they could shut down MedSite. |

## Areas of Concern

**Insiders Using Network Access**

Role-based access builds over time. Many staff members have access to too much information.

**Outsiders Using Network Access**

ABC Systems has access to PIDS and the network. Any deliberate or accidental acts by their staff could affect our ability to provide patient care if they modify or delete vital information on PIDS.

## 9.2 Risk Profile Worksheet for PIDS – Human Actors Using Physical Access

## Human Actors Using Physical Access

## Basic Risk Profile

**Step 12**

**Step 22**

**Threat**

*For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.*

*For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.*

**Impact Values**

*What is the potential impact on the organization in each applicable area?*

| Asset | Access | Actor | Motive | Outcome | Reputation | Financial | Productivity | Fines | Safety | Other |
|---|---|---|---|---|---|---|---|---|---|---|
| PIDS | physical | inside | accidental | disclosure | M | M | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |
| | | | deliberate | disclosure | M | M | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |
| | | outside | accidental | disclosure | H | H | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |
| | | | deliberate | disclosure | H | H | L | M | L | - |
| | | | | modification | M | M | M | M | H | - |
| | | | | loss, destruction | M | M | H | M | H | - |
| | | | | interruption | M | M | H | M | H | - |

**Basic Risk Profile**

**Human Actors Using Physical Access**

**Step 24**

**Probability**

*How likely is the threat to occur in the future? How confident are you in your estimate?*

**Step 26**

**Security Practice Areas**

*What is the stoplight status for each security practice area?*

**Step 27**

**Approach**

*What is your approach for addressing each risk?*

| Value | Confidence | Strategic | | | | | | Operational | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Very Somewhat Not At All | 1. Sec Training | 2. Sec Strategy | 3. Sec Mgmt | 4. Sec Policy & Reg | 5. Coll Sec Mgmt | 6. Cont Planning | 7. Phys Acc Cntrl | 8. Monitor Phys Sec | 9. Sys & Net Mgmt | 10. Monitor IT Sec | 11. Authen & Auth | 12. Vul Mgmt | 13. Encryption | 14. Sec Arch & Des | 15. Incident Mgmt | Accept | Defer | Mitigate |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | [✓ R] | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | □ | ☒ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | [✓ R] | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | □ | ☒ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | Y | [✓ R] | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | □ | ☒ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | ☒ | □ |
| L | \|----X\|------\| | R | R | R | Y | [✓ R] | Y | Y | [✓ R] | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | □ | ☒ |
| L | \|----X\|------\| | R | R | R | Y | [✓ R] | Y | Y | [✓ R] | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | □ | ☒ |
| L | \|----X\|------\| | R | R | R | Y | [✓ R] | Y | Y | [✓ R] | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | □ | ☒ |
| L | \|----X\|------\| | R | R | R | Y | [✓ R] | Y | Y | [✓ R] | ▨ | ▨ | ▨ | ▨ | ▨ | R | Y | □ | □ | ☒ |

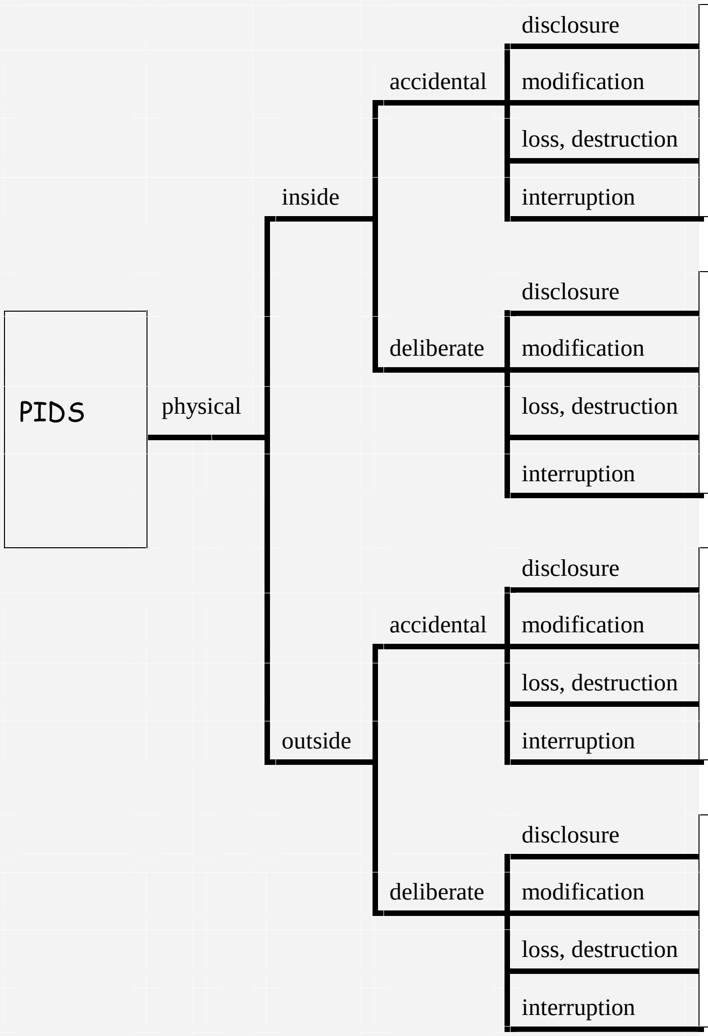
**Human Actors Using Physical Access**

**Threat Context**

**Step 13**

**Threat Actors**

*Which actors pose the biggest threats to this system via physical means?*



*Insiders acting accidentally:*

Staff using other people's computers

*Insiders acting deliberately:*

Disgruntled employees

*Outsiders acting accidentally:*

ABC Systems, patients

*Outsiders acting deliberately:*

Patients, terrorists, spies, vandals

## Threat Context

## Human Actors Using Physical Access

| Step 14 | | | | | | Step 15 | | | |
|---|---|---|---|---|---|---|---|---|---|
| Motive | | | | | | History | | | |
| *How strong is the actor's motive?* | | | *How confident are you in this estimate?* | | | *How often has this threat occurred in the past?* | *How accurate are the data?* | | |
| **High** | **Medium** | **Low** | **Very** | **Somewhat** | **Not At All** | | **Very** | **Somewhat** | **Not At All** |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __2___ times in __5___ years | ❑ | ☒ | ❑ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ❑ | ☒ | ❑ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ❑ | ☒ | ❑ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ❑ | ☒ | ❑ |
| ❑ | ☒ | ❑ | ❑ | ☒ | ❑ | __0___ times in __5___ years | ❑ | ❑ | ☒ |
| ❑ | ❑ | ☒ | ❑ | ☒ | ❑ | __0___ times in __5___ years | ❑ | ❑ | ☒ |
| ❑ | ❑ | ☒ | ❑ | ☒ | ❑ | __2___ times in __5___ years | ❑ | ❑ | ☒ |
| ❑ | ❑ | ☒ | ❑ | ☒ | ❑ | __0___ times in __5___ years | ❑ | ❑ | ☒ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ❑ | ❑ | ☒ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ❑ | ❑ | ☒ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ❑ | ❑ | ☒ |
| ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | __0___ times in __5___ years | ❑ | ❑ | ☒ |
| ❑ | ❑ | ☒ | ❑ | ☒ | ❑ | __0___ times in __5___ years | ❑ | ☒ | ❑ |
| ❑ | ❑ | ☒ | ❑ | ☒ | ❑ | __0___ times in __5___ years | ❑ | ☒ | ❑ |
| ❑ | ❑ | ☒ | ❑ | ☒ | ❑ | __1___ times in __5___ years | ❑ | ☒ | ❑ |
| ❑ | ❑ | ☒ | ❑ | ☒ | ❑ | __0___ times in __5___ years | ❑ | ☒ | ❑ |

**Step 16**

**Human Actors Using Physical Access** **Areas of Concern**

**Insiders Using Physical Access**

| | |
|---|---|
| Give examples of how *insiders acting accidentally* could use physical access to threaten this system. | |
| | |
| Give examples of how *insiders acting deliberately* could use physical access to threaten this system. | Any staff member can get physical access to PIDS by using PCs left unattended in exam rooms. PCs in exam rooms are typically left logged on to PIDS. |
| | Our main computer room is often left unlocked. Also, too many staff members seem to have keys to the room. Any staff member with malicious intent could gain access. |

**Outsiders Using Physical Access**

| | |
|---|---|
| Give examples of how *outsiders acting accidentally* could use physical access to threaten this system. | Any patient could accidentally see PIDS information when they are left alone in exam rooms. They could also deliberately look at PIDS information if they wanted to. |
| | ABC Systems has physical access all of our IT equipment. Any deliberate or accidental acts by their staff could affect our ability to provide patient care. |
| Give examples of how *outsiders acting deliberately* could use physical access to threaten this system. | Any patient could accidentally see PIDS information when they are left alone in exam rooms. They could also deliberately look at PIDS information if they wanted to. |
| | ABC Systems has physical access all of our IT equipment. Any deliberate or accidental acts by their staff could affect our ability to provide patient care. |

## Areas of Concern

| |
|---|
| **Insiders Using Physical Access** |
| |
| |
| |
| |
| **Outsiders Using Physical Access** |
| |
| |
| Terrorists and spies could attempt to physically access PIDS just as easily as they could try to hack it.  If they disrupt PIDS, they could shut down MedSite. |
| The PIDS server is located at ABC Systems' site.  Its staff has physical access to PIDS. Their physical security for the server is a concern. |

## 9.3 Risk Profile Worksheet for PIDS – System Problems

## System Problems

## Basic Risk Profile

**Step 12**

**Threat**

*For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.*

*For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.*

**Step 22**

**Impact Values**

*What is the potential impact on the organization in each applicable area?*

| Asset | Actor | Outcome | Reputation | Financial | Productivity | Fines | Safety | Other |
|---|---|---|---|---|---|---|---|---|
| PIDS | software defects | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | M | M | H | M | H | - |
| | | interruption | M | M | H | M | H | - |
| | system crashes | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | M | M | H | M | H | - |
| | | interruption | M | M | H | M | H | - |
| | hardware defects | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | M | M | H | M | H | - |
| | | interruption | M | M | H | M | H | - |
| | malicious code (virus, worm, Trojan horse, back door) | disclosure | H | H | L | M | L | - |
| | | modification | M | M | M | M | H | - |
| | | loss, destruction | M | M | H | M | H | - |
| | | interruption | M | M | H | M | H | - |

**Basic Risk Profile**

**Systems Problems**

**Step 24**

**Probability**

*How likely is the threat to occur in the future? How confident are you in your estimate?*

**Step 26**

**Security Practice Areas**

*What is the stoplight status for each security practice area?*

**Step 27**

**Approach**

*What is your approach for addressing each risk?*

| Value | Confidence | Strategic | | | | | | Operational | | | | | | | | | Approach | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Very Somewhat Not At All | 1. Sec Training | 2. Sec Strategy | 3. Sec Mgmt | 4. Sec Policy & Reg | 5. Coll Sec Mgmt | 6. Cont Planning | 7. Phys Acc Cntrl | 8. Monitor Phys Sec | 9. Sys & Net Mgmt | 10. Monitor IT Sec | 11. Authen & Auth | 12. Vul Mgmt | 13. Encryption | 14. Sec Arch & Des | 15. Incident Mgmt | Accept | Defer | Mitigate |
| | \|------\|------\| | | | | | | | ▨ | ▨ | | | ▨ | | ▨ | | | ❑ | ❑ | ❑ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | | | ▨ | | ▨ | | | ❑ | ❑ | ❑ |
| H | \|----X\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | ▨ | R | ▨ | R | Y | ❑ | ☒ | ❑ |
| H | \|X----\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | ▨ | R | ▨ | R | Y | ❑ | ☒ | ❑ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | | | | | ▨ | | | ❑ | ❑ | ❑ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | | | | | ▨ | | | ❑ | ❑ | ❑ |
| H | \|----X\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | ▨ | R | Y | ❑ | ☒ | ❑ |
| H | \|X----\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | ▨ | R | Y | ❑ | ☒ | ❑ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | | | ▨ | | ▨ | | | ❑ | ❑ | ❑ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | | | ▨ | | ▨ | | | ❑ | ❑ | ❑ |
| L | \|X----\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | ▨ | R | ▨ | R | Y | ❑ | ☒ | ❑ |
| L | \|X----\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | ▨ | R | ▨ | R | Y | ❑ | ☒ | ❑ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|------\|----X\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| L | \|----X\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |
| M | \|----X\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | Y | Y | R | R | R | R | Y | ❑ | ☒ | ❑ |

## System Problems

## Threat Context

**Step 15**

| | | | History | | | |
|---|---|---|---|---|---|---|
| | | | *How often has this threat occurred in the past?* | *How accurate are the data?* | | |
| | | | | **Very** | **Somewhat** | **Not At All** |
| PIDS | software defects | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | _10_ times in _1_ years | ❑ | ☒ | ❑ |
| | | interruption | _10_ times in _1_ years | ☒ | ❑ | ❑ |
| | system crashes | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | _10+_ times in _1_ years | ❑ | ☒ | ❑ |
| | | interruption | _10+_ times in _1_ years | ☒ | ❑ | ❑ |
| | hardware defects | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | _0_ times in _5_ years | ☒ | ❑ | ❑ |
| | | interruption | _0_ times in _5_ years | ☒ | ❑ | ❑ |
| | malicious code (virus, worm, Trojan horse, back door) | disclosure | _0_ times in _5_ years | ❑ | ❑ | ☒ |
| | | modification | _0_ times in _5_ years | ❑ | ❑ | ☒ |
| | | loss, destruction | _1_ times in _5_ years | ❑ | ☒ | ❑ |
| | | interruption | _2_ times in _1_ years | ❑ | ☒ | ❑ |

**Threat Context**

**System Problems**

**Notes**

*What additional notes about each threat do you want to record?*

Step 16

## System Problems

**Areas of Concern**

|  |  |
|---|---|
| **Software Defects** |  |
| Give examples of how *software defects* could threaten this system. | The PIDS database application locks up periodically. To get PIDS back up, we need to reboot the system. Anytime PIDS is down, it affects MedSite's ability to provide patient care. |
|  |  |
| **System Crashes** |  |
| Give examples of how *system crashes* could threaten this system. | PIDS has a history of crashing for a variety of reasons. Anytime PIDS is down, it affects MedSite's ability to provide patient care. |
|  |  |
| **Hardware Defects** |  |
| Give examples of how *hardware defects* could threaten this system. |  |
|  |  |
| **Malicious Code** |  |
| Give examples of how *malicious code* could threaten this system. (Consider viruses, worms, Trojan horses, back doors, others) | Any vulnerability could be exploited by a virus or other type of malicious code. |
|  |  |

**Areas of Concern**

| |
|---|
| **Software Defects** |
| |
| |
| **System Crashes** |
| |
| |
| **Hardware Defects** |
| |
| |
| **Malicious Code** |
| |
| Viruses are a major concern. PIDS was shut down twice last year because of virus problems. |

## 9.4 Risk Profile Worksheet for PIDS – Other Problems

## Other Problems

## Basic Risk Profile

**Step 12**

**Threat**

*For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.*

*For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.*

**Step 22**

**Impact Values**

*What is the potential impact on the organization in each applicable area?*

| Asset | Actor | Outcome | Reputation | Financial | Productivity | Fines | Safety | Other |
|---|---|---|---|---|---|---|---|---|
| PIDS | power supply problems | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | M | M | H | M | H | - |
| | | interruption | M | M | H | M | H | - |
| | telecommunications problems or unavailability | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | M | M | H | M | H | - |
| | third-party problems or unavailability of third-party systems | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | M | M | H | M | H | - |
| | natural disasters (e.g., flood, fire, tornado) | disclosure | H | H | L | M | L | - |
| | | modification | | | | | | |
| | | loss, destruction | M | M | H | M | H | - |
| | | interruption | M | M | H | M | H | - |

## Basic Risk Profile

## Other Problems

**Step 24**

**Probability**

*How likely is the threat to occur in the future? How confident are you in your estimate?*

**Step 26**

**Security Practice Areas**

*What is the stoplight status for each security practice area?*

**Step 27**

**Approach**

*What is your approach for addressing each risk?*

| Value | Confidence | Strategic | | | | | | Operational | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Very Somewhat Not At All | 1. Sec Training | 2. Sec Strategy | 3. Sec Mgmt | 4. Sec Policy & Reg | 5. Coll Sec Mgmt | 6. Cont Planning | 7. Phys Acc Cntrl | 8. Monitor Phys Sec | 9. Sys & Net Mgmt | 10. Monitor IT Sec | 11. Authen & Auth | 12. Vul Mgmt | 13. Encryption | 14. Sec Arch & Des | 15. Incident Mgmt | Accept | Defer | Mitigate |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| M | \|----X\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | Y | □ | ☒ | □ |
| M | \|X----\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | Y | □ | ☒ | □ |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| L | \|X----\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | Y | □ | ☒ | □ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| M | \|X----\|------\| | R | R | R | Y | R | Y | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | Y | □ | □ | ☒ |
| L | \|X----\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | □ | ☒ | □ |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | □ | ☒ | □ |
| L | \|X----\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | □ | ☒ | □ |
| L | \|X----\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | □ | ☒ | □ |

**Other Problems**

**Threat Context**

**Step 15**

**History**

| | | | *How often has this threat occurred in the past?* | *How accurate are the data?* | | |
|---|---|---|---|---|---|---|
| | | | | **Very** | **Somewhat** | **Not At All** |
| PIDS | power supply problems | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | __2___ times in __1___ years | ❑ | ☒ | ❑ |
| | | interruption | __2___ times in __1___ years | ☒ | ❑ | ❑ |
| | telecommunications problems or unavailability | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | interruption | __1___ times in __5___ years | ☒ | ❑ | ❑ |
| | third-party problems or unavailability of third-party systems | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | interruption | __3___ times in __2___ years | ☒ | ❑ | ❑ |
| | natural disasters (e.g., flood, fire, tornado) | disclosure | __0___ times in __5___ years | ☒ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | __2___ times in __5___ years | ☒ | ❑ | ❑ |
| | | interruption | __2___ times in __5___ years | ☒ | ❑ | ❑ |

**Threat Context**

**Other Problems**

**Notes**

*What additional notes about each threat do you want to record?*

Power supply is controlled by the site and its facilities group.

**Step 16**

## Other Problems

**Areas of Concern**

| Power Supply Problems | |
|---|---|
| Give examples of how *power supply problems* could threaten this system. | Power supply problems can lead to a denial of access to PIDS. Our backup procedures have failed in the past, so this is a concern. |
| | |

| Telecommunications Problems | |
|---|---|
| Give examples of how *telecommunications problems* could threaten this system. | We access PIDS using telecommunications lines. If there is a problem with any telecommunications equipment, then we could not access PIDS. |
| | |

| Third-Party Problems | |
|---|---|
| Give examples of how *third-party problems* could threaten this system. | MedSite is not a priority for ABC Systems. This prolongs downtime for PIDS. |
| | |

| Natural Disasters | |
|---|---|
| Give examples of how *natural disasters* could threaten this system. | MedSite is located on a flood plane. We have had a history of floods, especially in the past five years. Access to PIDS was interrupted each time. |
| | |

**Areas of Concern**

**Power Supply Problems**

**Telecommunications Problems**

**Third-Party Problems**

ABC Systems' configuration of our firewall restricts access to important Internet medical sites. They do not understand our requirements.

**Natural Disasters**

## Other Problems (cont.)

## Basic Risk Profile

**Step 12**

**Threat**

*For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.*

*For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.*

**Step 22**

**Impact Values**

*What is the potential impact on the organization in each applicable area?*

| **Asset** | **Actor** | **Outcome** | **Reputation** | **Financial** | **Productivity** | **Fines** | **Safety** | **Other** |
|---|---|---|---|---|---|---|---|---|
| PIDS | physical configuration or arrangement of buildings, offices, or equipment | disclosure | H | H | L | M | L | - |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | | | | | | |
| | | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | | | | | | |
| | | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | | | | | | |
| | | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | | | | | | |

## Basic Risk Profile

**Other Problems (cont.)**

**Step 24**

**Probability**

*How likely is the threat to occur in the future? How confident are you in your estimate?*

**Step 26**

**Security Practice Areas**

*What is the stoplight status for each security practice area?*

**Step 27**

**Approach**

*What is your approach for addressing each risk?*

| Value | Confidence | Strategic | | | | | | Operational | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Very<br>Somewhat<br>Not At All | 1. Sec Training | 2. Sec Strategy | 3. Sec Mgmt | 4. Sec Policy & Reg | 5. Coll Sec Mgmt | 6. Cont Planning | 7. Phys Acc Cntrl | 8. Monitor Phys Sec | 9. Sys & Net Mgmt | 10. Monitor IT Sec | 11. Authen & Auth | 12. Vul Mgmt | 13. Encryption | 14. Sec Arch & Des | 15. Incident Mgmt | Accept | Defer | Mitigate |
| H | \|X----\|------\| | R | R | R | Y | R | Y | Y | R | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | Y | □ | ☒ | □ |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |
| | \|------\|------\| | | | | | | | | | | | | | | | | □ | □ | □ |

**Other Problems (cont.)**

**Threat Context**

**Step 15**

| | | | History | | | |
|---|---|---|---|---|---|---|
| | | | *How often has this threat occurred in the past?* | *How accurate are the data?* | | |
| | | | | **Very** | **Somewhat** | **Not At All** |
| PIDS | physical configuration or arrangement of buildings, offices, or equipment | disclosure | 20+ times in 1 years | ☒ | □ | □ |
| | | modification | ______ times in ______ years | □ | □ | □ |
| | | loss, destruction | ______ times in ______ years | □ | □ | □ |
| | | interruption | ______ times in ______ years | □ | □ | □ |
| | | disclosure | ______ times in ______ years | □ | □ | □ |
| | | modification | ______ times in ______ years | □ | □ | □ |
| | | loss, destruction | ______ times in ______ years | □ | □ | □ |
| | | interruption | ______ times in ______ years | □ | □ | □ |
| | | disclosure | ______ times in ______ years | □ | □ | □ |
| | | modification | ______ times in ______ years | □ | □ | □ |
| | | loss, destruction | ______ times in ______ years | □ | □ | □ |
| | | interruption | ______ times in ______ years | □ | □ | □ |
| | | disclosure | ______ times in ______ years | □ | □ | □ |
| | | modification | ______ times in ______ years | □ | □ | □ |
| | | loss, destruction | ______ times in ______ years | □ | □ | □ |
| | | interruption | ______ times in ______ years | □ | □ | □ |

| Threat Context | Other Problems (cont.) |
|---|---|

| |
|---|
| **Notes** |
| *What additional notes about each threat do you want to record?* |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

**Step 16**

## Other Problems (cont.)

**Areas of Concern**

**Physical Configuration Problems**

| | |
|---|---|
| Give examples of how *physical configuration of buildings, offices, or equipment* could threaten this system. | Physical configuration of work areas permits unauthorized viewing of private patient information by staff members as well as outsiders. |
| | |

| | |
|---|---|
| Give examples of how<br>________________________<br>could threaten this system. | |
| | |

| | |
|---|---|
| Give examples of how<br>________________________<br>could threaten this system. | |
| | |

| | |
|---|---|
| Give examples of how<br>________________________<br>could threaten this system. | |
| | |

**Areas of Concern**

**Physical Configuration Problems**

# 10 Risk Profile Worksheet for ABC Systems – Other Problems

## Other Problems

## Basic Risk Profile

**Step 12**

**Threat**

*For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.*

*For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.*

**Step 22**

**Impact Values**

*What is the potential impact on the organization in each applicable area?*

| **Asset** | **Actor** | **Outcome** | **Reputation** | **Financial** | **Productivity** | **Fines** | **Safety** | **Other** |
|---|---|---|---|---|---|---|---|---|
| ABC Systems | key people taking a temporary leave of absence (e.g., due to illness, disability) | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | | | | | | |
| | key people leaving the organization permanently (e.g., retirement, other opportunities) | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | | | | | | |
| | threats affecting ~~a third-party or service provider~~ ABC Systems | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | L | L | L | L | L | - |
| | | disclosure | | | | | | |
| | | modification | | | | | | |
| | | loss, destruction | | | | | | |
| | | interruption | | | | | | |

**Basic Risk Profile**

**Other Problems**

**Step 24**

**Probability**

*How likely is the threat to occur in the future? How confident are you in your estimate?*

**Step 26**

**Security Practice Areas**

*What is the stoplight status for each security practice area?*

**Step 27**

**Approach**

*What is your approach for addressing each risk?*

| Value | Confidence | Strategic | | | | | | Operational | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Very<br>Somewhat<br>Not At All | 1. Sec Training | 2. Sec Strategy | 3. Sec Mgmt | 4. Sec Policy & Reg | 5. Coll Sec Mgmt | 6. Cont Planning | 7. Phys Acc Cntrl | 8. Monitor Phys Sec | 9. Sys & Net Mgmt | 10. Monitor IT Sec | 11. Authen & Auth | 12. Vul Mgmt | 13. Encryption | 14. Sec Arch & Des | 15. Incident Mgmt | Accept | Defer | Mitigate |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | ▨ | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | ▨ | | ▨ | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ❑ | ❑ | ❑ |
| L | \|--------\|------X\| | R | ▨ | R | ▨ | R | Y | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ☒ | ❑ | ❑ |
| | \|--------\|--------\| | | | | | | | | | | | | | | | | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | | | | | | | | | | | | | | | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | | | | | | | | | | | | | | | ❑ | ❑ | ❑ |
| | \|--------\|--------\| | | | | | | | | | | | | | | | | ❑ | ❑ | ❑ |

## Other Problems

## Threat Context

**Step 15**

| | | | History | | | |
|---|---|---|---|---|---|---|
| | | | *How often has this threat occurred in the past?* | *How accurate are the data?* | | |
| | | | | **Very** | **Somewhat** | **Not At All** |
| ABC Systems | key people taking a temporary leave of absence (e.g., due to illness, disability) | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | interruption | ______ times in ______ years | ❑ | ❑ | ❑ |
| | key people leaving the organization permanently (e.g., retirement, other opportunities) | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | interruption | ______ times in ______ years | ❑ | ❑ | ❑ |
| | threats affecting ~~a third-party or service provider~~ ABC Systems | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | interruption | __1___ times in __5___ years | ❑ | ❑ | ☒ |
| | | disclosure | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | modification | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | loss, destruction | ______ times in ______ years | ❑ | ❑ | ❑ |
| | | interruption | ______ times in ______ years | ❑ | ❑ | ❑ |

**Threat Context** **Other Problems**

**Notes**

*What additional notes about each threat do you want to record?*

To our knowledge, there has been one time that security issues affected ABC Systems' service in the last 5 years.

Step 16

## Other Problems

## Areas of Concern

### People Taking a Temporary Leave of Absence

| | |
|---|---|
| Give examples of how *key people taking a temporary leave of absence* could affect the ability of this person or group of people to provide critical services, skills, and knowledge. | |
| | |

### People Leaving the Organization Permanently

| | |
|---|---|
| Give examples of how *key people leaving the organization permanently* could affect the ability of this person or group of people to provide critical services, skills, and knowledge. | |
| | |

### Threats Affecting a Third-Party

| | |
|---|---|
| Give examples of how *threats affecting a third party or service provider* could affect the ability of that third party or service provider to provide critical services, skills, and knowledge. | ABC Systems configures and maintains all major systems and the network for MedSite. If ABC Systems is unable to provide services to MedSite because of threats to their systems and networks, MedSite's operations could be affected. |
| | |

| | |
|---|---|
| | |
| | |

**Areas of Concern**

**People Taking a Temporary Leave of Absence**

**People Leaving the Organization Permanently**

**Threats Affecting a Third-Party**

If there is a problem with PIDS or the network and ABC Systems is unable to respond in a timely manner, MedSite's downtime could be increased.

# 11 Network Access Paths Worksheet

## Steps 17 and 18

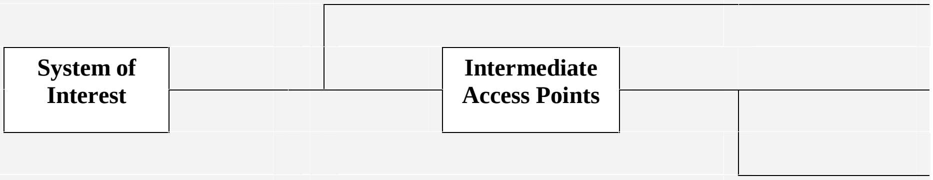
**Step 17**

**System of Interest**

*What system or systems are most closely related to the critical asset?*

PIDS (is its own system of interest)

**Access Points**



**Step 18a**

**System of Interest**

*Which of the following classes of components are part of the system of interest?*

☒ Servers
Server A

❑ Internal Networks

☒ On-Site Workstations
admin, physician, treatment room

❑ Others (list)

**Step 18b**

**Intermediate Access Points**

*Which of the following classes of components are used to transmit information and applications from the system of interest to people?*

*Which classes of components could serve as intermediate access points?*

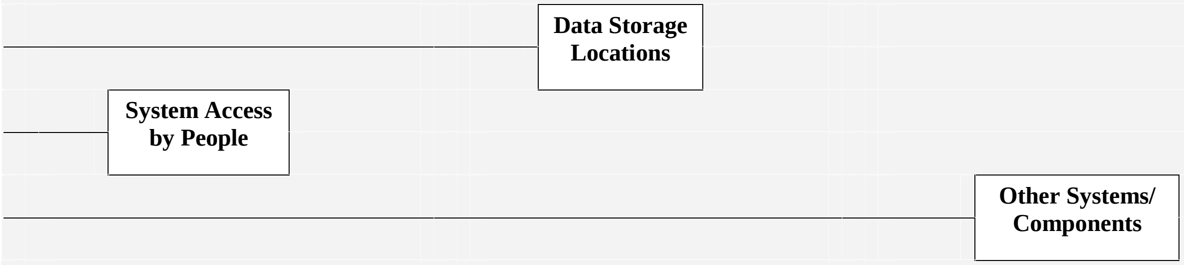
☒ Internal Networks

☒ External Networks

❑ Others (list)

Note: When you select a key class of components, make sure that you also document any relevant subclasses or specific examples when appropriate.

**Access Points**



**Step 18c**

**System Access by People**

*From which of the following classes of components can people (e.g., users, attackers) access the system of interest?*

*Consider access points both internal and external to your organization's networks.*

☒ On-Site Workstations

☒ Laptops
admin, physicians, IT

☒ PDAs/Wireless Components

☒ Home/External Workstations
physicians, senior admin

❑ Others (list)

**Step 18d**

**Data Storage Locations**

*On which classes of components is information from the system of interest stored for backup purposes?*

☒ Storage Devices
local backups, off-site tapes

❑ Others (list)

**Step 18e**

**Other Systems and Components**

*Which other systems access information or applications from the system of interest?*

*Which other classes of components can be used to access critical information or applications from the system of interest?*

☒ _____ECDS___________

☒ ____FRKS____________

☒ Most of the other systems

# 12 Infrastructure Review Worksheets

## Steps 19, 20,  and 21

*Note*
*In Step 19a, mark the path to each class selected in Steps 18a-18e.*

| Step 19a | Step 19b | | | | | Step 20 |
|---|---|---|---|---|---|---|
| **Class**<br>*Which classes of components are related to one or more critical assets?* | **Critical Assets**<br>*Which critical assets are related to each class?* | | | | | **Responsibility**<br>*Who is responsible for maintaining and securing each class of component?* |
| *(Document any relevant subclasses or specific examples when appropriate.)* | 1. PIDS | 2. paper med recs | 3. PCs | 4. ABC Systems | 5. ECDS | |
| Servers | | | | | | |
| Server A | ✓ | | ✓ | | | ABC Systems |
| Server B | | | ✓ | | ✓ | ABC Systems |
| | | | | | | |
| Internal Networks | | | | | | |
| All | ✓ | | ✓ | | ✓ | ABC Systems & our IT |
| | | | | | | |
| | | | | | | |
| On-Site Workstations | | | | | | |
| Admin | ✓ | | ✓ | | ✓ | ABC Systems & our IT |
| Physicians | ✓ | | ✓ | | ✓ | ABC Systems & our IT |
| Patient treatment rooms | ✓ | | ✓ | | ✓ | ABC Systems & our IT |
| Laptops | | | | | | |
| Admin | ✓ | | ✓ | | ✓ | ABC Systems & our IT |
| Physicians | ✓ | | ✓ | | ✓ | ABC Systems & our IT |
| IT | ✓ | | ✓ | | ✓ | ABC Systems & our IT |
| PDAs/Wireless Components | | | | | | |
| Physicians | ✓ | | | | | ABC Systems & our IT |
| Others | ✓ | | | | | ABC Systems & our IT |
| | | | | | | ABC Systems & our IT |

**Step 21**

<table>
<tr><th colspan="7">Protection</th><th>Notes/Issues</th></tr>
<tr><td colspan="4"><em>To what extent is security considered when configuring and maintaining each class of component?</em></td><td colspan="3"><em>How do you know?</em></td><td><em>What additional information do you want to record?</em></td></tr>
<tr><th>Very Much</th><th>Somewhat</th><th>Not At All</th><th>Don’t Know</th><th>Formal Techniques</th><th>Informal Means</th><th>Other</th><th></th></tr>
<tr><td colspan="8">Servers</td></tr>
<tr><td colspan="3">|-------------|---------------|</td><td>☒</td><td>❑</td><td>❑</td><td>❑</td><td></td></tr>
<tr><td colspan="3">|-------------|---------------|</td><td>☒</td><td>❑</td><td>❑</td><td>❑</td><td></td></tr>
<tr><td colspan="3">|-------------|---------------|</td><td>❑</td><td>❑</td><td>❑</td><td>❑</td><td></td></tr>
<tr><td colspan="8">Internal Networks</td></tr>
<tr><td colspan="3">|-------------|------X-------|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td>IT does some items on these.</td></tr>
<tr><td colspan="3">|-------------|---------------|</td><td>❑</td><td>❑</td><td>❑</td><td>❑</td><td></td></tr>
<tr><td colspan="3">|-------------|---------------|</td><td>❑</td><td>❑</td><td>❑</td><td>❑</td><td></td></tr>
<tr><td colspan="8">On-Site Workstations</td></tr>
<tr><td colspan="3">|----------X-|---------------|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td>IT focuses on Admin’s workstations.</td></tr>
<tr><td colspan="3">|-------------|--X-----------|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td></td></tr>
<tr><td colspan="3">|-------------|--X-----------|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td></td></tr>
<tr><td colspan="8">Laptops</td></tr>
<tr><td colspan="3">|-------------|---------------|</td><td>☒</td><td>❑</td><td>❑</td><td>❑</td><td></td></tr>
<tr><td colspan="3">|-------------|--X-----------|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td></td></tr>
<tr><td colspan="3">|--X---------|---------------|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td>IT does a lot of extras on their own PCs.</td></tr>
<tr><td colspan="8">PDAs/Wireless Components</td></tr>
<tr><td colspan="3">|-------------|-------------X|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td>No one has paid attention to this.</td></tr>
<tr><td colspan="3">|-------------|-------------X|</td><td>❑</td><td>❑</td><td>☒</td><td>❑</td><td></td></tr>
<tr><td colspan="3">|-------------|---------------|</td><td>❑</td><td>❑</td><td>❑</td><td>❑</td><td></td></tr>
</table>

*Note*

*In Step 19a, mark the path to each class selected in Steps 18a-18e.*

| Step 19a | Step 19b | | | | | Step 20 |
|---|---|---|---|---|---|---|
| **Class** | **Critical Assets** | | | | | **Responsibility** |
| *Which classes of components are related to one or more critical assets?* | *Which critical assets are related to each class?* | | | | | *Who is responsible for maintaining and securing each class of component?* |
| *(Document any relevant subclasses or specific examples when appropriate.)* | 1. PIDS | 2. paper med recs | 3. PCs | 4. ABC Systems | 5. ECDS | |
| Other Systems | | | | | | |
| All other systems | ✓ | | ✓ | | ✓ | ABC Systems and our IT |
| | | | | | | |
| | | | | | | |
| Storage Devices | | | | | | |
| Local back-up | ✓ | | ✓ | | ✓ | ABC Systems and our IT |
| Off-site tapes | ✓ | | | | ✓ | Not sure |
| | | | | | | |
| External Networks | | | | | | |
| All | ✓ | | | | | Unknown |
| | | | | | | |
| | | | | | | |
| Home/External Workstations | | | | | | |
| Physicians, senior admin. | ✓ | | | | | Individual |
| | | | | | | |
| | | | | | | |
| Other __________________ | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Step 21**

| Protection | | Notes/Issues |
|---|---|---|
| *To what extent is security considered when configuring and maintaining each class of component?* | *How do you know?* | *What additional information do you want to record?* |

| Very Much<br>Somewhat<br>Not At All | Don't Know | Formal Techniques | Informal Means | Other | |
|---|---|---|---|---|---|

Other Systems

| | | | | | |
|---|---|---|---|---|---|
| \|-------------\|---------X----\| | □ | □ | ☒ | □ | |
| \|-------------\|---------------\| | □ | □ | □ | □ | |
| \|-------------\|---------------\| | □ | □ | □ | □ | |

Storage Devices

| | | | | | |
|---|---|---|---|---|---|
| \|-------------\|---------------\| | ☒ | □ | □ | □ | |
| \|-------------\|---------------\| | ☒ | □ | □ | □ | Might be outsourced from ABC Systems |
| \|-------------\|---------------\| | □ | □ | □ | □ | |

External Networks

| | | | | | |
|---|---|---|---|---|---|
| \|-------------\|---------------\| | ☒ | □ | □ | □ | |
| \|-------------\|---------------\| | □ | □ | □ | □ | |
| \|-------------\|---------------\| | □ | □ | □ | □ | |

Home/External Workstations

| | | | | | |
|---|---|---|---|---|---|
| \|-------------\|---------------\| | ☒ | □ | □ | □ | Up to owner to manage |
| \|-------------\|---------------\| | □ | □ | □ | □ | |
| \|-------------\|---------------\| | □ | □ | □ | □ | |

Other ___________________

| | | | | | |
|---|---|---|---|---|---|
| \|-------------\|---------------\| | □ | □ | □ | □ | |
| \|-------------\|---------------\| | □ | □ | □ | □ | |
| \|-------------\|---------------\| | □ | □ | □ | □ | |

# 13 Probability Evaluation Criteria Worksheet

## Step 23

**Step 23**

**Frequency-Based Criteria**

1. *Think about what constitutes a high, medium, and low likelihood of occurrence for threats to your organization’s critical assets.*

| | High | | | | Medium |
|---|---|---|---|---|---|
| **Time Between Events** | Daily | Weekly | Monthly | Four Times Per Year | < 4 Times Per Year<br>~~Two Times Per Year~~ |
| **Annualized Frequency** | 365 | 52 | 12 | 4 | ~~2~~<br>< 4 |

2. *Draw lines that separate high from medium and medium from low.*

| Medium | Low | | | | |
|---|---|---|---|---|---|
| One Time Per Year | < 1 Time Per Year<br>~~Once Every Two Years~~ | Once Every Five Years | Once Every 10 Years | Once Every 20 Years | Once Every 50 Years |
| 1 | ~~0.5~~<br>< 1 | 0.2 | 0.1 | 0.05 | 0.02 |

# 14 Protection Strategy Worksheet

## Steps 25, 29

This section includes an excerpt of the entire protection strategy for MedSite. Two types of practice areas are included: the selected mitigation areas and a few of the other practice areas with general, strategic improvements.

The mitigation areas reflect corporate or strategic-level changes driven primarily by the mitigation plans for specific risks to critical assets. The mitigation areas are

- Security awareness and training
- Collaborative security management
- Monitoring and auditing physical security
- Authentication and authorization

Strategic level changes were also identified for the rest of the security practice areas. The other areas with strategic changes included here are security policies and regulations.

## 14.1 Protection Strategy for Security Awareness and Training

## 1. Security Awareness and Training

**Stoplight Status** R

*Step 25: How formal is your organization's training strategy?*

*Step 29: Will any mitigation activities change your training strategy?*
*Do you want to make any additional changes to your training strategy?*

| **Training Strategy** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has a documented training strategy that includes security awareness training and security-related training for supported technologies. | ☐ Current | ☐ Change |
| The organization has an informal and undocumented training strategy. | ☒ Current | ☐ Change |
| ____________________________________________<br>____________________________________________ | ☐ Current | ☐ Change |

*Step 25: How often is security awareness training provided?*

*Step 29: Will any mitigation activities change how often security awareness training is provided?*
*Do you want to make any additional changes to how often security awareness training is provided?*

| **Security Awareness Training** | **Step 25** | **Step 29** |
|---|---|---|
| Periodic security awareness training is provided for all employees ____1____time(s) every ____1____ years. | ☐ Current | ☒ Change |
| Security awareness training is provided for new staff members as part of their orientation activities. | ☒ Current | ☐ Change |
| The organization does not provide security awareness training. Staff members learn about security issues on their own. | ☐ Current | ☐ Change |
| ____________________________________________<br>____________________________________________ | ☐ Current | ☐ Change |

## 1. Security Awareness and Training

*Step 25: To what extent are IT staff members required to attend security-related training?*

*Step 29: Will any mitigation activities change the requirement for attending security-related training?*
*Do you want to make any additional changes to the requirement for attending security-related training?*

| **Security-Related Training for Supported Technologies** | **Step 25** | **Step 29** |
|---|---|---|
| Information technology staff members are required to attend security-related training for any technologies that they support. | □ Current | □ Change |
| Information technology staff members can attend security-related training for any technologies that they support if they request it. | □ Current | ☒ Change |
| The organization generally does not provide opportunities for information technology staff members to attend security-related training for supported technologies. Information technology staff members learn about security-related issues on their own. | ☒ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |

*Step 25: How formal is your organization's mechanism for providing periodic security updates?*

*Step 29: Will any mitigation activities change your mechanism for providing periodic security updates?*
*Do you want to make any additional changes to your mechanism for providing periodic security updates?*

| **Periodic Security Updates** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has a formal mechanism (including coordination with ABC Systems) for providing staff members with periodic updates/bulletins about important security issues. | □ Current | ☒ Change |
| The organization does not have a mechanism for providing staff members with periodic updates/bulletins about important security issues. | ☒ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |

## 1. Security Awareness and Training

**Stoplight Status** R

*Step 25: How formal is your organization's mechanism for verifying that staff receives training?*

*Step 29: Will any mitigation activities change your mechanism for verifying that staff receives training?*
*Do you want to make any additional changes to your mechanism for verifying that staff receives training?*

| **Training Verification** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has formal mechanisms for tracking and verifying that staff members receive appropriate security-related training. | □ Current | □ Change |
| The organization has informal mechanisms for tracking and verifying that staff members receive appropriate security-related training. | □ Current | ☒ Change |
| The organization has no mechanisms for tracking and verifying that staff members receive appropriate security-related training. | ☒ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

*Step 25: What additional characteristic of your current approach to security awareness and training do you want to record?*

*Step 29: Will any mitigation activities change this characteristic?*
*Do you want to make any additional changes to this characteristic?*

| **Other:** | **Step 25** | **Step 29** |
|---|---|---|
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

## 14.2 Protection Strategy for Collaborative Security Management

## 5. Collaborative Security Management

**Stoplight Status** R

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **collaborators and partners**?*

*Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with collaborators and partners?*
*Do you want to make any additional changes to the policies and procedures for protecting information when working with collaborators and partners?*

| **Collaborators and Partners** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has documented policies and procedures for protecting information when working with collaborators and partners. | □ Current | □ Change |
| The organization has documented policies and procedures for protecting certain information when working with collaborators and partners. The organization has informal and undocumented policies and procedures for protecting other types of information when working with collaborators and partners. | □ Current | □ Change |
| The organization has informal and undocumented policies and procedures for protecting information when working with collaborators and partners. | ☒ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **contractors and subcontractors**?*

*Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with contractors and subcontractors?*
*Do you want to make any additional changes to the policies and procedures for protecting information when working with contractors and subcontractors?*

| **Contractors and Subcontractors** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has documented policies and procedures for protecting information when working with contractors and subcontractors. | □ Current | □ Change |
| The organization has documented policies and procedures for protecting certain information when working with contractors and subcontractors. The organization has informal and undocumented policies and procedures for protecting other types of information when working with contractors and subcontractors. | □ Current | □ Change |
| The organization has informal and undocumented policies and procedures for protecting information when working with contractors and subcontractors. | ☒ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |

## 5. Collaborative Security Management

*Step 25: How formal are your organization's policies and procedures for protecting information when working with* ***service providers****?*

*Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with service providers?*
*Do you want to make any additional changes to the policies and procedures for protecting information when working with service providers?*

| **Service Providers** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has documented policies and procedures for protecting information when working with service providers. | □ Current | □ Change |
| The organization has documented policies and procedures for protecting certain information when working with service providers. The organization has informal and undocumented policies and procedures for protecting other types of information when working with service providers. | □ Current | □ Change |
| The organization has informal and undocumented policies and procedures for protecting information when working with service providers. | ☒ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

*Step 25: To what extent does your organization formally communicate its information protection requirements to third parties?*

*Step 29: Will any mitigation activities change how your organization communicates its information protection requirements to third parties?*
*Do you want to make any additional changes to how your organization communicates its information protection requirements to third parties?*

| **Requirements** | **Step 25** | **Step 29** |
|---|---|---|
| The organization documents information protection requirements and explicitly communicates them to all appropriate third parties. | □ Current | □ Change |
| The organization informally communicates information protection requirements to ~~all appropriate third parties~~. Facilities Management and ABC Systems. | □ Current | ☒ Change |
| The organization does not communicate information protection requirements to third parties. | ☒ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

## 5. Collaborative Security Management

**Stoplight Status** R

*Step 25: To what extent does your organization verify that third parties are addressing information protection requirements?*

*Step 29: Will any mitigation activities change verification mechanisms?*
*Do you want to make any additional changes to verification mechanisms?*

| **Verification** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements. | □ Current | □ Change |
| The organization has informal mechanisms for verifying that ~~all third-party organizations, outsourced security services, mechanisms, and technologies~~ Facilities Management and ABC Systems meet its needs and requirements. | □ Current | ☒ Change |
| The organization has no mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements. | ☒ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

*Step 25: To what extent does your security-awareness training program include information about collaborative security management?*

*Step 29: Will any mitigation activities change the content of your security awareness training to include information about collaborative security management?*
*Do you want to make any additional changes to the content of your security awareness training?*

| **Staff Awareness** | **Step 25** | **Step 29** |
|---|---|---|
| The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for all employees _________time(s) every _________ years. | □ Current | □ Change |
| The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for new staff members as part of their orientation activities. | □ Current | □ Change |
| The organization's security-awareness training program does not include information about the organization's collaborative security management policies and procedures. Staff members learn about collaborative security management policies and procedures on their own. | ☒ Current | □ Change |
| ____________________________________________ | □ Current | □ Change |

## 5. Collaborative Security Management

*Step 25: What additional characteristic of your current approach to collaborative security management do you want to record?*

*Step 29: Will any mitigation activities change this characteristic?*
*Do you want to make any additional changes to this characteristic?*

| **Other:** | **Step 25** | **Step 29** |
|---|---|---|
| ____________________<br>____________________ | □ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |

## 14.3 Protection Strategy for Monitoring and Auditing Physical Security

## 8. Monitoring and Auditing Physical Security

**Stoplight Status** R

*Step 25: Who is currently responsible for monitoring and auditing physical security?*

*Step 29: Will any mitigation activities change responsibility for monitoring and auditing physical security?*
*Do you want to make any additional changes affecting responsibility for monitoring and auditing physical security?*

| **Responsibility** | **Step 25** | | | **Step 29** | | |
|---|---|---|---|---|---|---|
| | ☒ Current | | | ☐ Change | | |
| Task | Internal | External | Combined | Internal | External | Combined |
| Keeping maintenance records to document repairs and modifications to IT hardware | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Monitoring physical access to controlled IT hardware | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Monitoring physical access to controlled IT software media | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Monitoring physical access to restricted work areas | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Reviewing monitoring records on a periodic basis | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Investigating and addressing any unusual activity that is identified | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

## 8. Monitoring and Auditing Physical Security

*Step 25: To what extent are procedures for this area formally documented?*

*Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?
Do you want to make any additional changes to how procedures are documented for this area?*

| Procedures | Step 25 | Step 29 |
|---|---|---|
| ***If staff from your organization is partly or completely responsible for this area:*** | | |
| The organization has formally documented plans and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media. | □ Current | □ Change |
| The organization has some formally documented policies and procedures for monitoring physical access to ~~the building and premises, work areas~~, IT hardware, and software media. Some policies and procedures in this area are informal and undocumented. | □ Current | ☒ Change |
| The organization has informal and undocumented plans and procedures for monitoring physical access to ~~the building and premises, work areas~~, IT hardware, and software media. | ☒ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

*Step 25: To what extent are staff members required to attend training in this area?*

*Step 29: Will any mitigation activities change the requirement for attending training in this area?
Do you want to make any additional changes to the requirement for attending training in this area?*

| Training | Step 25 | Step 29 |
|---|---|---|
| ***If staff from your organization is partly or completely responsible for this area:*** | | |
| Designated staff members are required to attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media. | □ Current | □ Change |
| Designated staff members can attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media if they request it. | □ Current | □ Change |
| The organization generally does not provide opportunities for designated staff members to attend training for monitoring physical access to ~~the building and premises, work areas~~, IT hardware, and software media. Designated staff members learn about monitoring physical access on their own. | ☒ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

## 8. Monitoring and Auditing Physical Security

**Stoplight Status** R

**Third Party A:** Facilities Management

*Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?*

*Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?*

| **Collaborative Issues** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media. | □ Current | □ Change |
| The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, ~~IT hardware, and software media~~. | □ Current | ☒ Change |
| The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, ~~IT hardware, and software media.~~ | ☒ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |

*Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?*

*Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?*

| **Verification** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security. | □ Current | □ Change |
| The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security. | □ Current | ☒ Change |
| The organization does not verify that contractors and service providers have met the requirements for monitoring physical security. | ☒ Current | □ Change |
| ____________________<br>____________________ | □ Current | □ Change |

## 8. Monitoring and Auditing Physical Security

**Third Party B:___________________________________**

*Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?*

*Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?*

| **Collaborative Issues** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media. | □ Current | □ Change |
| The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media. | □ Current | □ Change |
| The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media. | □ Current | □ Change |
| ____________________________________________________________<br>____________________________________________________________ | □ Current | □ Change |

*Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?*

*Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?*

| **Verification** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security. | □ Current | □ Change |
| The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security. | □ Current | □ Change |
| The organization does not verify that contractors and service providers have met the requirements for monitoring physical security. | □ Current | □ Change |
| ____________________________________________________________<br>____________________________________________________________ | □ Current | □ Change |

## 14.4 Protection Strategy for Authentication and Authorization

## 11. Authentication and Authorization

**Stoplight Status** R

*Step 25: Who is currently responsible for authentication and authorization?*

*Step 29: Will any mitigation activities change responsibility for authentication and authorization?*
*Do you want to make any additional changes affecting responsibility for authentication and authorization?*

| | | | | | | |
|---|---|---|---|---|---|---|
| **Responsibility** | **Step 25** | | | **Step 29** | | |
| | ☒ Current | | | ☒ Change | | |
| Task | Internal | External | Combined | Internal | External | Combined |
| Implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections | ☐ | ☒ | ☐ | ☐ | ☐ | ☒ |
| Implementing user authentication (e.g., passwords, biometrics) to restrict user access to information, sensitive systems, specific applications and services, and network connections | ☐ | ☒ | ☐ | ☐ | ☐ | ☒ |
| Establishing and terminating access to systems and information for both individuals and groups | ☐ | ☐ | ☒ | ☐ | ☐ | ☒ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ____________________ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

## 11. Authentication and Authorization

*Step 25: To what extent are procedures for this area formally documented?*

*Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?
Do you want to make any additional changes to how procedures are documented for this area?*

| **Procedures** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from your organization is partly or completely responsible for this area:*** | | |
| The organization has formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections. | □ Current | □ Change |
| The organization has some formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections. Some procedures in this area are informal and undocumented. | □ Current | ☒ Change |
| The organization has informal and undocumented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections. | ☒ Current | □ Change |
| ____________________________________________<br>____________________________________________ | □ Current | □ Change |

*Step 25: To what extent are staff members required to attend training in this area?*

*Step 29: Will any mitigation activities change the requirement for attending training in this area?
Do you want to make any additional changes to the requirement for attending training in this area?*

| **Training** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from your organization is partly or completely responsible for this area:*** | | |
| Information technology staff members are required to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections. | □ Current | □ Change |
| Information technology staff members can attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections if they request it. | □ Current | ☒ Change |
| The organization generally does not provide opportunities for information technology staff members to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections. Information technology staff members learn about authentication and authorization on their own. | ☒ Current | □ Change |
| ____________________________________________ | □ Current | □ Change |

## 11. Authentication and Authorization

**Stoplight Status** R

**Third Party A:** ABC Systems

*Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?*

*Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?*

| **Collaborative Issues** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services. | □ Current | □ Change |
| The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks. | □ Current | ☒ Change |
| The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks. | ☒ Current | □ Change |
| ______________________________<br>______________________________ | □ Current | □ Change |

*Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?*

*Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to you verify that requirements are being met?*

| **Verification** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization. | □ Current | □ Change |
| The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization. | □ Current | ☒ Change |
| The organization does not verify that contractors and service providers have met the requirements for authentication and authorization. | ☒ Current | □ Change |
| ______________________________<br>______________________________ | □ Current | □ Change |

## 11. Authentication and Authorization

**Third Party B:**___________________________________

*Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?*

*Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party?*
*Do you want to make any additional changes to how you communicate requirements to this third party?*

| **Collaborative Issues** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services. | □ Current | □ Change |
| The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks. | □ Current | □ Change |
| The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks. | □ Current | □ Change |
| ____________________________________________________________<br>____________________________________________________________ | □ Current | □ Change |

*Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?*

*Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area?*
*Do you want to make any additional changes to you verify that requirements are being met?*

| **Verification** | **Step 25** | **Step 29** |
|---|---|---|
| ***If staff from a third party is partly or completely responsible for this area:*** | | |
| The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization. | □ Current | □ Change |
| The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization. | □ Current | □ Change |
| The organization does not verify that contractors and service providers have met the requirements for authentication and authorization. | □ Current | □ Change |
| ____________________________________________________________<br>____________________________________________________________ | □ Current | □ Change |

## 14.5 Protection Strategy for Security Policies and Regulations

## 4. Security Policies and Regulations

**Stoplight Status** y

*Step 25: To what extent are your organization's security-related policies formally documented?*

*Step 29: Will any mitigation activities change the extent to which your security-related policies are formally documented? Do you want to make any additional changes to the extent to which your security-related policies are formally documented?*

| **Documented Policies** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has a comprehensive set of formally documented security-related policies. | ☐ Current | ☐ Change |
| The organization has a partial set of formally documented security-related policies. Some security-related policies are informal and undocumented. | ☒ Current | ☐ Change |
| The organization's security-related policies are informal and undocumented. | ☐ Current | ☐ Change |
| ____________________<br>____________________ | ☐ Current | ☐ Change |

*Step 25: How formal is your organization's mechanism for creating and updating its security-related policies?*

*Step 29: Will any mitigation activities change how your security-related policies are created and updated? Do you want to make any additional changes to how your security-related policies are created and updated?*

| **Policy Management** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has a formal mechanism for creating and updating its security-related policies. | ☐ Current | ☐ Change |
| The organization has a formal mechanism for creating its security-related policies. The organization has an informal and undocumented mechanism for updating its security-related policies. | ☐ Current | ☐ Change |
| The organization has an informal and undocumented mechanism for creating and updating its security-related policies. | ☒ Current | ☐ Change |
| ____________________<br>____________________ | ☐ Current | ☐ Change |

## 4. Security Policies and Regulations

*Step 25: How formal are your organization's procedures for enforcing its security-related policies?*

*Step 29: Will any mitigation activities change how security-related policies are enforced?*
*Do you want to make any additional changes to how security-related policies are enforced?*

| Policy Enforcement | Step 25 | Step 29 |
|---|---|---|
| The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are consistently followed. | ❑ Current | ❑ Change |
| The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are inconsistently followed. | ❑ Current | ☒ Change |
| The organization has informal and undocumented procedures for enforcing its security-related policies. | ☒ Current | ❑ Change |
| ____________________________________________<br>____________________________________________ | ❑ Current | ❑ Change |

*Step 25: To what extent does your security-awareness training program include information about the organization's security policies and regulations?*

*Step 29: Will any mitigation activities change the content of your security awareness training to include security policy and regulation information?*
*Do you want to make any additional changes to the content of your security awareness training?*

| Staff Awareness | Step 25 | Step 29 |
|---|---|---|
| The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for all employees ____1____time(s) every ____1____ years. | ❑ Current | ☒ Change |
| The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for new staff members as part of their orientation activities. | ❑ Current | ❑ Change |
| The organization's security-awareness training program does not include information about the organization's security policies and regulations. Staff members learn about security policies and regulations on their own. | ☒ Current | ❑ Change |
| ____________________________________________<br>____________________________________________ | ❑ Current | ❑ Change |

## 4. Security Policies and Regulations

**Stoplight Status** Y

*Step 25: How formal are your organization's procedures for complying with security-related policies and regulations?*

*Step 29: Will any mitigation activities change how your organization complies with security-related policies and regulations?*
*Do you want to make any additional changes to how your organization complies with security-related policies and regulations?*

| **Policy and Regulation Compliance** | **Step 25** | **Step 29** |
|---|---|---|
| The organization has formal procedures for complying with information security policies, applicable laws and regulations, and insurance requirements. | ☐ Current | ☐ Change |
| The organization has formal procedures for complying with certain information security policies, applicable laws and regulations, and insurance requirements. Some procedures in this area are informal and undocumented. | ☐ Current | ☒ Change |
| The organization has informal and undocumented procedures for complying with information security policies, applicable laws and regulations, and insurance requirements. | ☒ Current | ☐ Change |
| ____________________<br>____________________ | ☐ Current | ☐ Change |

*Step 25: What additional characteristic of your current approach to security policies and regulations do you want to record?*

*Step 29: Will any mitigation activities change this characteristic?*
*Do you want to make any additional changes to this characteristic?*

| **Other:** | **Step 25** | **Step 29** |
|---|---|---|
| ____________________<br>____________________ | ☐ Current | ☐ Change |
| ____________________<br>____________________ | ☐ Current | ☐ Change |
| ____________________<br>____________________ | ☐ Current | ☐ Change |

# 15 Mitigation Plan Worksheet

## Step 28

**Mitigation Area:** 1. Security Awareness and Training

**Step 28**

| **Mitigation Activity** | **Rationale** |
|---|---|
| *Which mitigation activities are you going to implement in this security practice area?* | *Why did you select each activity?* |
| Provide periodic security awareness training for all employees once a year.<br>Note: This will change MedSite's protection strategy. | MedSite's current policy is to provide awareness training for new employees only. This is inadequate. Security awareness training should be provided on a periodic basis. |
| Enable IT staff members to attend security-related training for any technologies that they support. | The security practices survey indicated that there is a lack of training for IT staff at MedSite. |
| The manager in each department will keep a list of people who have received security awareness training and when they received it. | We must set up a tracking mechanism if we intend to improve our training related to security. |

| **Mitigation Responsibility** | **Additional Support** |
|---|---|
| *Who needs to be involved in implementing each activity? Why?* | *What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?* |
| MedSite's senior management team and the training department manager | Increasing the frequency of security awareness training requires commitment and funding from senior management. It will also require a commitment from MedSite's Training Department. |
| MedSite's IT manager must take responsibility for implementing this mitigation activity. | MedSite's senior managers must approve and find funding for this activity. MedSite's CIO needs to sponsor implementation of this activity. |
| The manager in each MedSite department | Each department manager must participate in this activity. Senior managers need to make this a requirement for it to work. |

**Mitigation Area:** __5. Collaborative Security Management_________________

**Step 28**

| **Mitigation Activity** | **Rationale** |
|---|---|
| *Which mitigation activities are you going to implement in this security practice area?* | *Why did you select each activity?* |
| Designate an IT staff member as point of contact to communicate our requirements for protecting PIDS information to ABC Systems.<br>Designate staff member from the Maintenance Department to communicate our physical security requirements for building security to the Facilities Management Group.<br>Note: This will change MedSite's protection strategy. | We are currently doing nothing with respect to communicating security requirements to ABC Systems and the Facilities Management Group. Establishing a point of contact for each organization should improve communication of our requirements. |
| The IT point of contact will verify that requirements for protecting PIDS information are met by ABC Systems.<br>The Maintenance Department point of contact will verify that requirements for physical security are met by the Facilities Management Group for the building.<br>Note: This will change MedSite's protection strategy. | If we are establishing a means to communicate our requirements to ABC Systems and the Facilities Management Group, then we need the points of contact to make sure that those requirements have been met. |
| Contract with ABC Systems to send security bulletins to MedSite's IT point of contact, who will forward the bulletins to MedSite's staff. | MedSite's staff is not receiving information about security problems, such as viruses. |

| **Mitigation Responsibility** | **Additional Support** |
|---|---|
| *Who needs to be involved in implementing each activity? Why?* | *What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?* |
| TBD – Responsibility must be assigned by MedSite's CIO and the manager of the Maintenance Department. | MedSite's senior management team must sponsor this activity. The CIO and manager of the Maintenance Department must assign the points of contact. |
| TBD – A point of contact must be assigned to work with ABC Systems. A point of contact must be assigned to work with the Facilities Management Group. | MedSite's senior management team must sponsor this activity. The CIO and manager of the Maintenance Department must assign the points of contact. |
| TBD – A point of contact must be assigned to work with ABC Systems. | MedSite's senior management team must sponsor this activity. The CIO must assign the point of contact. |

**Mitigation Area:** __8. Monitoring and Auditing Physical Security___________

**Step 28**

| **Mitigation Activity** | **Rationale** |
|---|---|
| *Which mitigation activities are you going to implement in this security practice area?* | *Why did you select each activity?* |
| Document formal procedures for monitoring physical access to all IT hardware and software media.<br>Note: This will change MedSite's protection strategy. | Some staff members from MedSite's IT department informally monitor the physical security of IT hardware and software. Formalizing the procedures would help to ensure that they are consistently applied by all IT staff members. |
| Assign a point of contact from MedSite to work with the Facilities Management Group to monitor physical access to the building and premises. The point of contact will be responsible for <u>communicating</u> MedSite's requirements for monitoring physical security and for <u>verifying</u> that the requirements have been met.<br>Note: This will change MedSite's protection strategy. | Responsibility for monitoring and auditing physical security is assigned to the Facilities Management Group and MedSite. Activities are not coordinated among the two organizations. Establishing points of contact at MedSite to work with staff from the Facilities Management Group should improve communication of our requirements and improve how physical security is managed. |
| | |

| **Mitigation Responsibility** | **Additional Support** |
|---|---|
| *Who needs to be involved in implementing each activity? Why?* | *What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?* |
| TBD – A small team to document the procedures must be assigned by MedSite's CIO and/or IT manager. | MedSite's CIO must sponsor this activity and assign a small team to document the procedures. |
| TBD – A point of contact must be assigned to work with Facilities Management Group. | MedSite's senior management team must sponsor this activity. The manager of the Maintenance Department must assign the points of contact. |
| | |

**Mitigation Area:** __11. Authentication and Authorization________________

**Step 28**

| Mitigation Activity | Rationale |
|---|---|
| *Which mitigation activities are you going to implement in this security practice area?* | *Why did you select each activity?* |
| Assign joint responsibility for the following to MedSite and ABC Systems.<br>– implementing access controls for PIDS<br>– implementing user authentication for PIDS<br>Note: This will change MedSite's protection strategy. | People from MedSite's IT department must participate in controlling access to PIDS. Staff at ABC Systems do not know who should have legitimate access to what. |
| Document procedures for controlling access to PIDS.<br>Note: This will change MedSite's protection strategy. | Restricting user access is currently done in an ad hoc manner. MedSite's IT department must develop formalized procedures for restricting user access to ensure that they are consistently applied by all IT staff members. Procedures for implementing access controls must specify how to work with staff from ABC Systems. |
| Assign a point of contact from MedSite to work with ABC Systems to control access to PIDS. The point of contact will be responsible for communicating MedSite's requirements for controlling access to PIDS and for verifying that the requirements have been met.<br>Note: This will change MedSite's protection strategy. | We are currently doing nothing with respect to communicating requirements to ABC Systems for controlling access to information and systems. Establishing a point of contact from MedSite's IT department should improve communication of our requirements. |

| **Mitigation Responsibility** | **Additional Support** |
|---|---|
| *Who needs to be involved in implementing each activity? Why?* | *What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?* |
| TBD – A point of contact must be assigned to work with ABC Systems. | MedSite's senior management team must sponsor this activity. The CIO must assign staff to work with ABC Systems. |
| TBD – A small team to document the procedures must be assigned by MedSite's CIO and/or IT manager. The team should include representation from the IT department and the point of contact for ABC Systems. | MedSite's senior management team must sponsor this activity. MedSite's CIO must sponsor this activity and assign a small team to document the procedures. |
| TBD – A point of contact must be assigned to work with ABC Systems. | MedSite's senior management team must sponsor this activity. The CIO must assign the point of contact. |

**Mitigation Area:** __11. Authentication and Authorization (cont.)__________________

**Step 28**

| **Mitigation Activity** | **Rationale** |
|---|---|
| *Which mitigation activities are you going to implement in this security practice area?* | *Why did you select each activity?* |
| Check all PIDS workstations in treatment rooms to ensure that access to those workstations automatically times out after a designated period of time. | Too many people, both staff and patients, have physical access to PIDS from workstations in treatment rooms. Unauthorized people could use this access to view a patient's medical records deliberately. Or a patient could accidentally see another patient's medical records. Privacy regulations makes this an important issue. |
| | |
| | |

| **Mitigation Responsibility** | **Additional Support** |
|---|---|
| *Who needs to be involved in implementing each activity? Why?* | *What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?* |
| TBD – MedSite’s CIO and/or IT manager will identify the IT staff who will implement this activity. Designated staff will have to work with staff from ABC Systems to set automatic timeouts. | MedSite’s senior management team must sponsor this activity. MedSite’s CIO must sponsor this activity and assign a staff to set automatic timeouts. |
| | |
| | |

**Mitigation Area:** __4. Security Policies and Regulations__________________

**Step 28**

| **Mitigation Activity** | **Rationale** |
|---|---|
| *Which mitigation activities are you going to implement in this security practice area?* | *Why did you select each activity?* |
| Create procedures for complying with HIPAA data security regulations.<br>Note: This will change MedSite's protection strategy. | MedSite has two years in which to be in compliance with the HIPAA data security requirements.<br>Note: This activity is driven by the regulations rather than any specific risk. |
| Include information about MedSite's security-related policies and procedures in the new security awareness training.<br>Note: This will change MedSite's protection strategy. | Few staff members are aware of or understand MedSite's security-related policies. This information must be featured in awareness training.<br>Note: This activity is driven by general concerns rather than any specific risk. |
| Procedures for enforcing MedSite's security-related policies must be created.<br>Note: This will change MedSite's protection strategy. | People's behaviors related to security will only change if they understand that management strictly enforces MedSite's security policies.<br>Note: This activity is driven by general concerns rather than any specific risk. |

| **Mitigation Responsibility** | **Additional Support** |
|---|---|
| *Who needs to be involved in implementing each activity? Why?* | *What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?* |
| TBD – Responsibility must be assigned by MedSite's senior management team. | MedSite's senior management team must sponsor this activity. |
| MedSite's senior management team and the Training Department manager | Updating the content of security awareness training requires commitment and funding from senior management. It will also require a commitment from MedSite's Training Department. |
| MedSite's senior management team | MedSite's senior management team must sponsor this activity. |

# 16 Next Steps Worksheet

## Step 30

**Step 30**

**Management Sponsorship for Security Improvement**

*What must management do to support the implementation of OCTAVE-S results?*

Consider:

- Contribute funds to information security activities.
- Assign staff to information security activities.
- Ensure that staff members have sufficient time allocated to information security activities.
- Enable staff to receive training about information security.
- Make information security a strategic priority.

MTF management must

- allocate funds to implement the mitigation plans
- make information security a strategic priority

All functional managers must ensure that staff members have sufficient time to participate in any security-related activities to which they are assigned.

**Monitoring Implementation**

*What will the organization do to track progress and ensure that the results of this evaluation are implemented?*

Each team assigned responsibility for a risk mitigation plan will be responsible for scheduling and implementing that plan. Each team will provide a written status report prior to the monthly management team meeting.

**Expanding the Current Information Security Risk Evaluation**

*Will you expand the current OCTAVE-S evaluation to include additional critical assets? Which ones?*

No, but we will review all deferred risks within the next 30 days to see if anything else needs to be done for them. We will also do a gap analysis between the results of OCTAVE-S and current regulations (including HIPAA) and see if there are any other required practices that we should consider during another round of resource allocations in the next quarter.

**Next Information Security Risk Evaluation**

*When will the organization conduct its next OCTAVE-S evaluation?*

The next OCTAVE-S evaluation will be performed 12-15 months from now.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY
(Leave Blank)

2. REPORT DATE
January 2005

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
OCTAVE-S Implementation Guide, Version 1.0, Volume 10

5. FUNDING NUMBERS
F19628-00-C-0003

6. AUTHOR(S)
Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2003-HB-003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization’s security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization’s personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization’s unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization’s business and security processes, so it will be able to conduct all activities by itself.

14. SUBJECT TERMS
information security, risk management, OCTAVE

15. NUMBER OF PAGES
198

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL